INFORMATIKA V JAVNI UPRAVI 2016

5. - 6. december 2016
Kongresni center Brdo pri Kranju

Zavarujemo aktivni imenik pred zlorabami

Robert Bergles, UnistarPRO d.o.o.
Lana Berden, MZZ

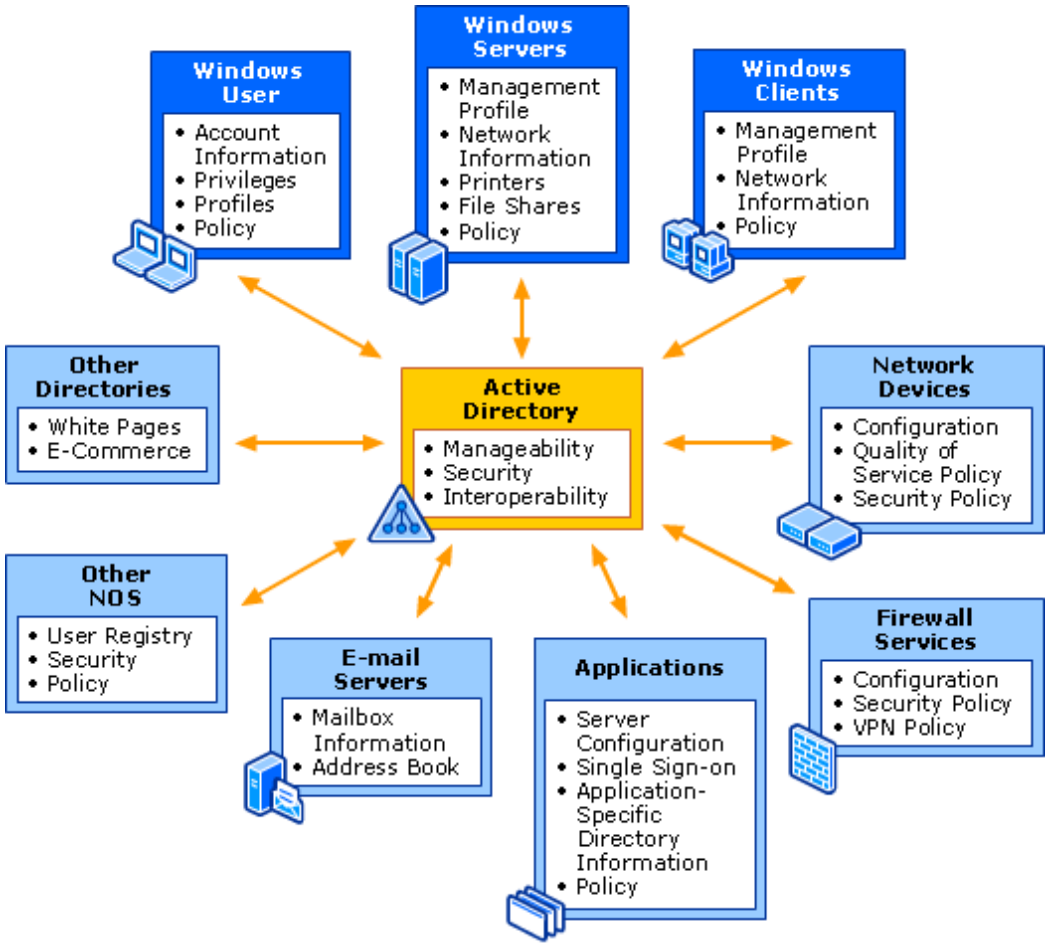
6.12.2016

- 21+ let v IT
- 10 let skrbnik sistemov v javni upravi.
- Varnostni pregled in optimizacija aktivnega imenika .
- Implementacija varnosti končnih odjemalcev 802.1x.
- Upravljanje javnih in hibridnih oblakov z Azure.
- Arhitekt storitev prehoda v Microsoft Office 365.
- Upravljanje naprav z Intune MDM.
- Arhitekt sistemov z visoko razpoložljivostjo.
- Uporaba System center orodij 2007 in 2012 R2 SCOM, SCCM,..

Agenda

- **Hacking.**
  - Prevzem **lokalnih admin pravic** na delovni postaji.
  - Prevzem **domain admin pravic** na domeni
- Analiza varnostnih lukenj in rešitev, da se zgornja incidenta ne zgodita.
- Varnostni pregled aktivnega imenika.
- Optimizacija GPO objektov.
- Health Check aktivnega imenika.
- Zavarovanje multifunkcijskih naprav.
- Analiza licenc in optimizacija licenciranja.
- Primer dobre prakse; **Optimizacija aktivnega imenika MZZ (Lana Berden)**

Zakaj se odločiti za optimizacijo in varnostni pregled **Aktivnega imenika**



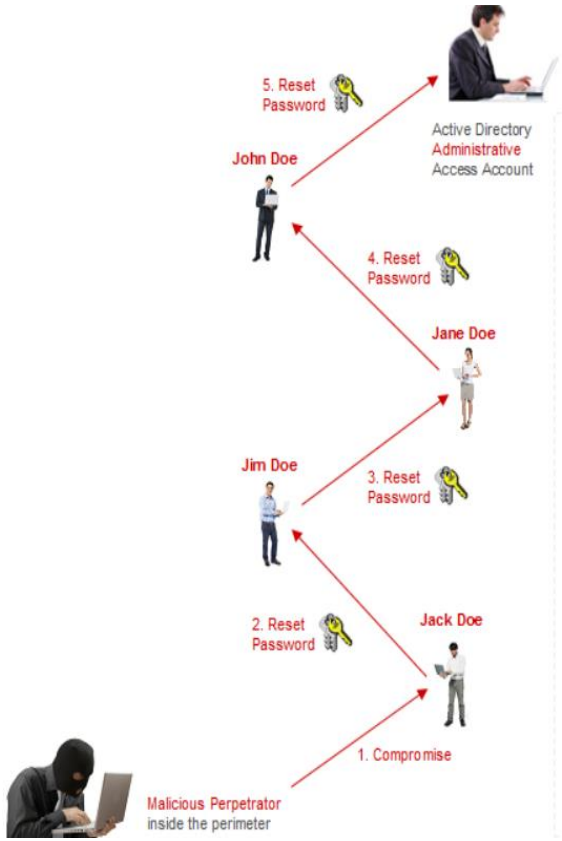
Top pet odgovorov pri pregledu ADja

- Imamo Backup.
- Nismo urgenca.
- Od viška glava ne boli.
- Za vsak slučaj.
- Za rezervo če se kaj sesuje.
- …..

ABC preprečevanja osnovnih **zlorab**

- Omejite dostop do **zagonskega menija** v BIOSu.
- Omogočite **maksimalni User Account** control zaščito.
- Razmejite **privilegije** za upravljanje delovnih postaj in strežnikov.
- Omogočite **BITLocker** na vseh delovnih postajah.
- Omogočite beleženje **Privilege of USE.**
- …..

Varnostni pregled aktivnega imenika



Cilj varnostnega pregleda aktivnega imenika je**, odkritje varnostnih lukenj za potencialne vdore ter zavarovanje imeniških podpornih storitev pred zlorabo,** glede na Microsoftova priporočila ter uveljavljanje dobre prakse.

Potencialne grožnje v aktivnem imeniku TOP 10

1. **Izmenjava uporabniških računov in gesel.**
2. **Opuščanje nadgradenj avtentikacijskih protokolov, „*ne vem kaj bo nehalo delovati*“.**
3. **Upravljanje strežnikov in delovnih postaj z enotnim admin uporabnikom.**
4. **Pozabljeni „*kao*“ začasni visoko privilegirani računi, „*ne vem na kaj je vezan račun*“.**
5. **Uporabniki s previsokimi lokalnimi privilegiji, „*samo da imam mir*“.**
6. Pomanjkljivo spremljanje varnostnih dogodkov potencialnih groženj.
7. Opuščanje požarnih pregrad „*samo da dela*“.
8. Pozabljeni računi testnega ali pilotskega projekta v produkciji.
9. Opuščanje varnih kriptirnih protokolov zaradi kompleksnosti izvedbe.
10. Rutinska in nepremišljena dejanja skrbnikov.

Varnostni pregled **TOP 10**

1. Koliko uporabniških računov ima pravice domenskih administratorjev ?
2. Ali še vedno uporabljate stare podedovane avtentikacijske protokole za prijavo NT 4.0?
3. Kako upravljate z revizijskimi sledmi in kdo ima dostop do njih?
4. Ali imajo vsi administratorji vklopljen maksimalen UAC ?
5. Kako upravljate izjeme Windows Firewall na delovnih postajah in strežnikih?
6. Koliko privilegiranih računov ima nastavljeno „password never expires“ ?
7. Koliko skrbnikov se je zamenjalo?
8. Koliko imate neaktivnih računov ?
9. Kako nadzirate skrbnike ?
10. Kako beležite spremembe dogodkov „change management“ v aktivnem imeniku

Optimizacija Group policy objektov

Cilj optimizacije GPO objektov je **zmanjšanje in racionalizacija števila GPO objektov** ter po principu dobre prakse nastaviti arhitekturo za enostavno obvladovanje nastavitev.

Optimizacija GPO **TOP 10**

1. Koliko imate GPO objektov?
2. Kdaj ste nazadnje posodobili varnostne nastavitve za IE, *IE 8.0*?
3. Koliko GPO objektov je neučinkovitih zaradi zastarelosti oziroma naj ostanejo, *za vsak slučaj* ?
4. Kdaj ste nazadnje posodobili GPO varnostne nastavitve za novejše operacijske sisteme ? *XP* ?
5. Kdo ima pravico upravljati z GPO objekti ?
6. Koliko GPO objektov je dedicirano samo na uporabnika, namesto na skupino ?
7. Koliko imate izjem in nastavitev Enforce ?
8. Kako imate porazdeljene nastavitve za računalnike in uporabnike ?
9. V koliko GPO objektih imate nastavljene varnostne nastavitve ?
10. Kako dokumentirate spremembe ?

Health check aktivnega imenika

Cilj pregleda zdravja aktivnega imenika je **analiza fizičnih objektov na vseh domenskih strežnikih**, konsistenčnost baz ter analiza replikacij med njimi.

Health check **TOP 10**

1. Kdaj ste nazadnje preverili replikacijo med Dcji ?
2. Ali so baze NTDS.dit približno enako velike ?
3. Ali imajo vsi Dcji enake GPO Objekte v sysvol mapi?
4. Kdaj ste nazadnje defragmentirali bazo NTDS.dit ?
5. Kdaj ste nazadnje preverili DFS replikacijo?
6. Kako je z replikacijo DNS zapisov med Dcji?
7. Kako se porazdeljene vloge in funkcije med Dcji?
8. Kako zagotavljate disaster recovery aktivnega imenika?
9. Ali res izkoriščate vse zmožnosti GPO objektov novih OS?
10. Kako urejujete revizijske sledi „Event log“ ?

Optimizacija in varnostni pregled DNS

Optimizacija ter zavarovanje DNS storitve je pomembna zaradi potencialnih **preprostih načinov vdorov** ter optimalnega naslavljanja med domenami in poddomenami.

Optimizacija in varnostni pregled DNS **TOP 10**

1. Kako imate zavarovan vpis v DNS bazo, „*vse dela Windows*“ ?
2. Koliko imate neaktivnih zapisov ?
3. Kako zagotavljate disaster recovery za DNS strežnike, „*je del aktivnega imenika*“?
4. Kako imate zasnovano replikacijo DNS zapisov med strežniki, „*vsi vse*“?
5. Kdo ima pravico upravljati DNS strežnike?
6. Koliko imate podvojenih zapisov ?
7. Ali ste preverili kako varen je strežnik s katerim replicirate podatke ?
8. Kako zagotavljate varnost internih zapisov?
9. Ali ste pomislili na uporabo DNSSec?
10. Kako dokumentirate spremembe ?

Zavarovanje multifunkcijskih naprav

Cilj zavarovanja multifunkcijskih naprav je preprečitev **posrednih dostopov do dokumentov** ki se nahajajo na pomnilnikih v multifunkcijski napravi ter preprečitev nepooblaščenega dostopa do naprave za tiskanje ali skeniranje.

Zavarovanje multifunkcijskih naprav

TOP 10

1. Ali lahko naprava neposredno dostopa do Interneta?
2. Ali ima naprava trajni pomnilnik ali disk za shranjevanje dokumentov?
3. Katere protokole imate nastavljene za upravljanje tiskalnikov ?
4. Ali redno in sproti brišete disk na napravi ?
5. Ali ste uvedli enkripcijo za komunikacijo ?
6. Kdaj ste nazadnje posodobili mikrokodo naprave ?
7. Kdo ima pravico upravljanja tiskalnikov?
8. Ali ste onemogočili nepotrebne protokole ?
9. Ali beležite kateri dokumenti se tiskajo ?
10. Ali ste spremenili public comunity name za SNMP V2, oziroma izbrali varen SNMP V3

Analiza licenc (SAM)

Z analizo in optimizacijo licenc, poskušamo doseči **optimalno uporabo licenc ter zmanjšanja stroškov** glede na dinamično spreminjanje poslovanja podjetja in Microsoft licenciranja.

Kako razumemo licenčno izrazoslovje

- Full Packaged Product (Fpp).
- Software Assurance.
- Open Value.
- Enterprise Agreement.
- External Connector Licensing.
- Per Processor Licensing.
- Server License And Cals.
- Standard And Enterprise Cals.
- Management Licensing.
- Online Services.

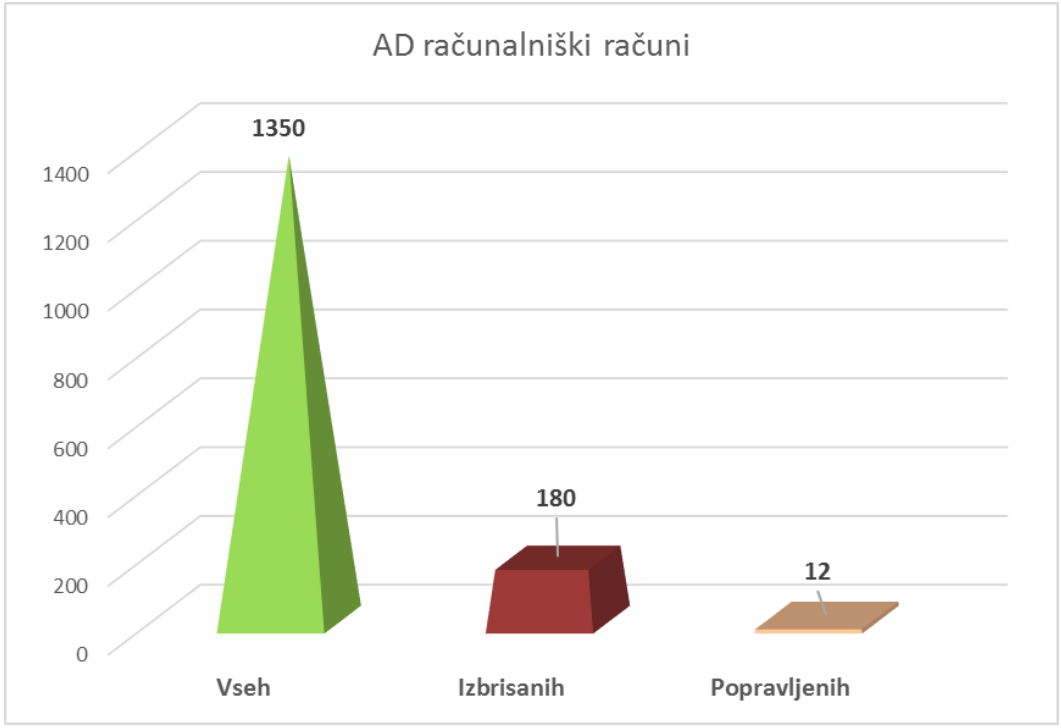
Zakaj SAM **TOP 10 ?**

1. Poiščite najbolj optimalno vrsto licenciranja glede na vaše potrebe.
2. Odkrijete programsko opremo, ki ne sme biti nameščena.
3. Najdite in upokojite operacijske sisteme, ki ogrožajo varnost vašega sistema.
4. Pridobite evidenco strojne in programske opreme.
5. Na podlagi analize poenotite programsko opremo.
6. Primerjajte kupljeno in nameščeno programsko opremo.
7. Standardizirajte dokumentacijo o licencah v digitalni obliki.
8. Opustite zastarelo opremo.
9. Imejte nadzor nad nameščeno programsko opremo.
10. Izognite se globi in sramoti za uporabo nelegalne opreme.

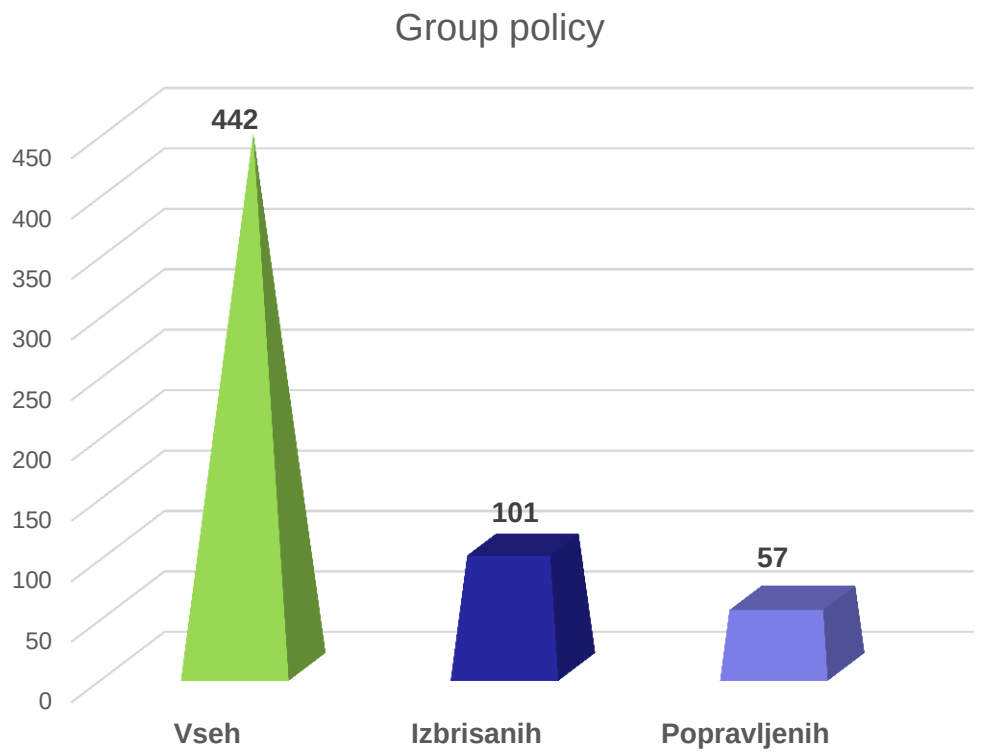
Primer dobre prakse (Mzz Lana Berden)

- Varnostni pregled ter Health check AD.
- Optimizacija GPO.
- Optimizacija DNS.
- Zavarovanje multifunkcijskih naprav.
- Analiza in optimizacija Microsoft licenc.

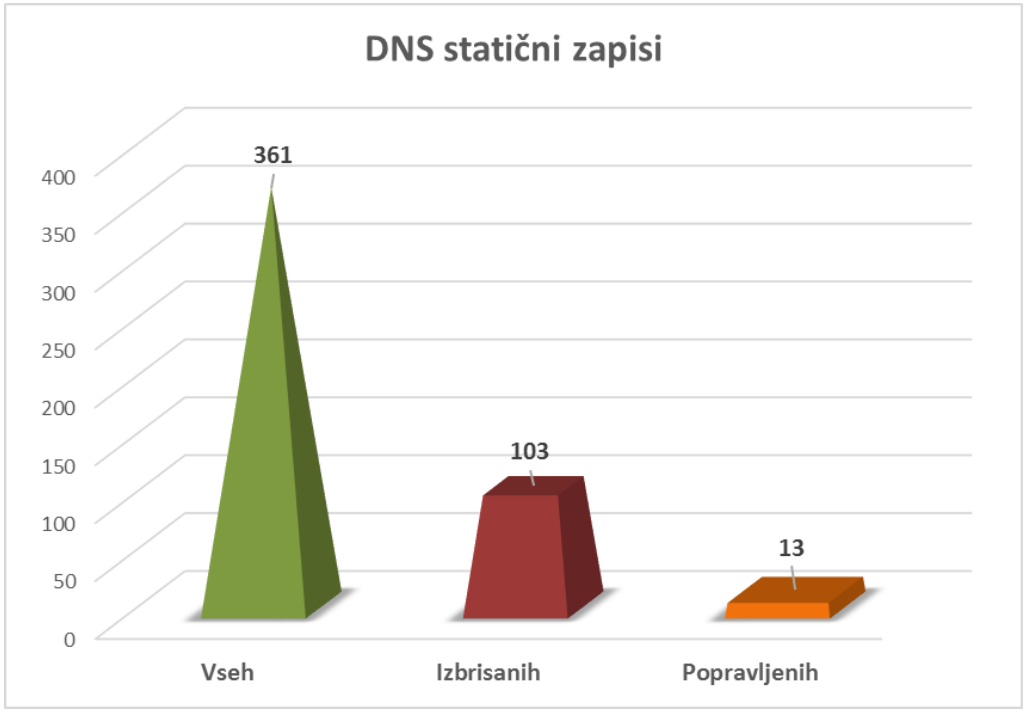
Aktivni imenik objekti



Group Policy



DNS


DNS statični zapisi
361
103
13
400
350
300
250
200
150
100
50
0
Vseh
Izbrisanih
Popravljenih

Hvala za vašo pozornost !

Vprašanja?

Pripombe?

Predlogi?