INFORMATIKA V JAVNI UPRAVI 2015

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

Informatika v javni upravi 2015

"Odprimo digitalni potencial javne uprave"

PRIVILEGIRANI DOSTOPI IN VARNOST AKTIVNEGA IMENIKA

Halis Tabaković, Alenka Glas, FMC d.o.o.

16.12.2015

slovensko društvo informatika

www.iju2015.si

Predstavitev avtorjev

Halis Tabaković, Vodja oddelka Microsoft

- 10 let na področju informatike
- Microsoft Specialist, MTA, MCITP, MCSE
- Aktivni imenik, Hyper-V, PowerShell, SCCM, SCOM

Alenka Glas, Svetovalka za področje varnosti

- 20 let na področju varovanja informacij
- Vodilna presojevalka (lead auditor) ISO/IEC 27001
- Vodilna presojevalka (lead auditor) ISO 22301

Domenske storitve in Aktivni imenik

Ključni del IT infrastrukture

- Hierarhična pregledna struktura
- Centralizirana administracija
- Visoka razpoložljivost storitve
- Delegiranje pravic
- Zaupanja
- Skupinske politike

Pregled in optimizacija Aktivnega imenika

- Kako skrbite za varnost Aktivnega imenika?
- Katero verzijo (nivo gozda, domene) Aktivnega imenika uporabljate?
  Zakaj? Ali uporabljate vse funkcionalnosti te verzije?
- Kateri uporabniki imajo več pravic in kakšne pravice imajo?
  Kako nadzirate te uporabnike? Kako zagotavljate revizijske sledi?
- Katere storitve tečejo na domenskih kontrolerjih?
- Koliko imate neaktivnih računov (uporabniki, računalniki)?
- Koliko imate skupin in kako jih uporabljate?
- Kakšno politiko gesel imate?
- Ali imate urejene skupinske politike?
- Ali imate dokumentiran Aktivni imenik?

Pomen informacij v sodobni družbi

Sodobna družba temelji na informacijah

Informacije so premoženje vsake sodobne organizacije

Elektronsko poslovanje je omogočilo nove poslovne poti, ki se zanašajo na učinkovit program za varovanje informacij, s katerim si lahko podjetje pridobi zaupanje strank… (Marko Potokar)

Varnost informacijskega sistema

Ob pridobitvi administratorskega dostopa do Aktivnega imenika, uporabnik lahko dostopa skoraj do vseh virov znotraj organizacije.

Napadi na računalniške infrastrukture so vse bolj pogosti, zato je ključnega pomena, da te vire pravilno zaščitimo.

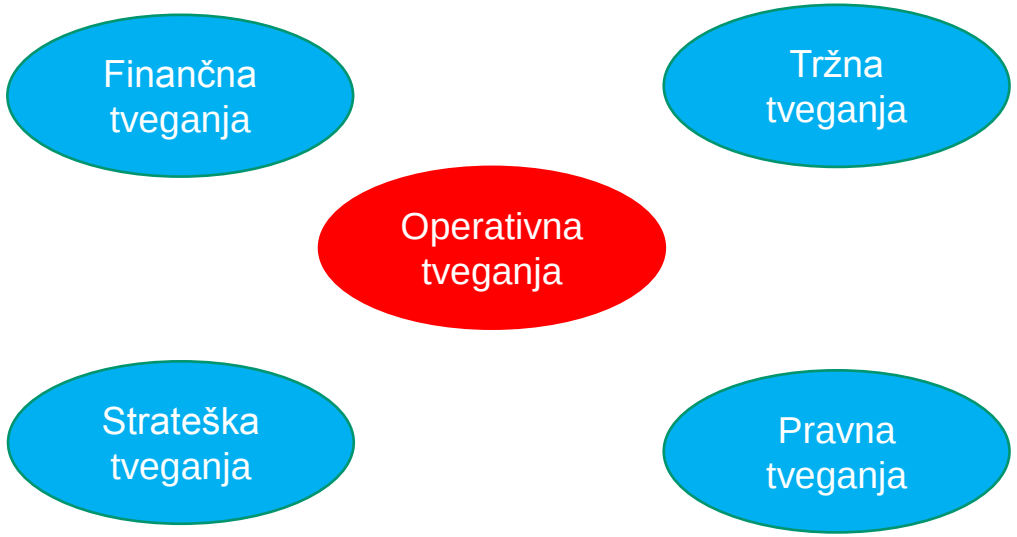
Povprečen čas za odkritje vdora je več kot 6 mesecev.

SUVI

Osnovna načela varovanja informacij v organizacijah:

- C confidentiality zaupnost
- I integrity celovitost
- A availability razpoložljivost

Varovanje informacij temelji na zmanjševanju tveganj.



Grožnje, ranljivosti

Grožnja

Najverjetnejši povod izvršenega varnostnega dogodka, ki lahko povzroči izpad delovanja ali napačno delovanje dela ali celotnega sistema oziroma poslovnega procesa.

Ranljivost

Pomanjkljivost sredstva (vira) ali skupine sredstev, ki jo lahko izkoristi ena ali več groženj.

Upravljanje dostopnih pravic

Najpomembnejša kontrola varovanja informacij

Upravljanje dostopnih pravic je torej:

- omejitev dostopa do informacij na najmanjši obseg, ki je potreben za izvedbo poslovnega procesa oziroma za zagotavljanje storitve
- dodelitev edinstvenega uporabniškega imena vsaki osebi, ki ima dostop do informacij
- omejitev fizičnega dostopa do prostorov in informacij

Privilegirani dostopi

Se obravnavajo kot vsi ostali dostopi

Tveganja so ista, njihova velikost pa bistveno večja, saj izraba takih pooblastil lahko povzroči velike posledice:

	Uporabniški dostopi	Privilegirani dostopi	
Grožnje	V	V	Verjetnost
Ranljivosti	M	V	Posledica
Tveganje	S	V	Tveganje

Pregled in optimizacija Aktivnega imenika

- Dokumentacija obstoječega stanja
- Analiza Aktivnega imenika za potencialne vdore in varnostne pomanjkljivosti
- Zagotavljanje revizijskih sledi
- Priporočila in optimizacija skupinskih politik
- Priprava načrta DRP (Disaster recovery plan)

Hvala za vašo pozornost !