INFORMATIKA V JAVNI UPRAVI 2015

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

Informatika v javni upravi 2015

"Odprimo digitalni potencial javne uprave"

Informacijska varnost v državni upravi

Damjan Križman

16.12.2015

slovensko društvo informatika

www.iju2015.si

Informacijska varnost v državni upravi skozi čas

- **V 70-tih in 80-tih letih:** veliki samostojni sistemi, malo komunikacij, veliki stroški, profesionalnost IT ekip, zagotavljanje zanesljivosti delovanja in razpoložljivosti sistemov, manj ogrožanja pred vdori.
- **Sredi 80-tih in v 90-tih letih:** prodor osebnih računalnikov, širjenje dostopnosti informacijskih tehnologij, pojav in širjenje škodljive programske opreme ter povečanih varnostnih groženj, ki se stopnjuje z uporabo in dostopnostjo interneta.
- **90-ta leta:** zavedanje o varnostnih grožnjah in varovanju podatkov bolj ali manj prepuščeno IT kadrom, management pogosto povezuje pojem varnosti s sistemom bivše države.
- **Po letu 2000:** naraščanje zavedanja pomena informacijske varnosti z začetkom vključevanja v NATO in EU, predvsem v povezavi z varovanjem tajnih podatkov.
- **Danes:** z razvojem informacijske tehnologije in njeno vključenostjo v vsakodnevno življenje in procese je informacijska varnost vpeta v sisteme in družbo na vseh ravneh.

Aktualna problematika

- **Državne institucije in svetovno gospodarstvo delujejo le na podlagi vedno bolj avtomatiziranih informacijskih procesov**, daljinskih dostopov in upravljanj ter prenosov podatkov po globalnih komunikacijskih omrežjih, zato so tudi vse kritične državne in meddržavne infrastrukture podvržene grožnjam in poskusom napadov.
- **Pojavljajo se nove in tehnološko vse bolj dovršene varnostne grožnje**, ki so pogosto odraz tako notranjih kot zunanjih političnih razmer ter organiziranega kriminala.
- **Podatki in informacije**, ki se hranijo v informacijskih sistemih ali se prenašajo znotraj informacijskih sistemov in po informacijskih omrežjih, **so izpostavljeni najrazličnejšim nevarnostim**, kot so nepooblaščen dostop do podatkov in informacij, nepooblaščena uporaba, prisvojitev, sprememba, poneverba ali uničenje, pa tudi prenos škodljive programske kode in zavrnitev storitve.
- **Informacijski sistemi in njihovi uporabniki se stalno srečujejo s težavami, kot sta neželena elektronska pošta in škodljiva programska oprema**, v katero spadajo vohunska programska oprema, trojanski konji, virusi, črvi itd.
- **Uporaba škodljive programske opreme za gradnjo omrežij iz okuženih računalnikov**, namenjenih nezakoniti uporabi, nezakonitemu pridobivanju podatkov, kraji identitete, zbiranju uporabnikovih življenjskih in nakupovalnih navad s sledenjem uporabe interneta, sovražnemu govoru, otroški pornografiji itd.
- **Za delovanje države je zato zelo pomembna ustrezna organizacija informacijske varnosti**, tako v smislu postavitve varnostnih pravil in ozaveščanja uporabnikov informacijskih tehnologij na vseh nivojih, kot hitrega odzivanja na varnostne grožnje.

Trenutno stanje na področju informacijske varnosti v DU

- **večji in podatkovno-varnostno bolj izpostavljeni organi so bolje ekipirani**, imajo na voljo relativno večja finančna sredstva, varnostna ozaveščenost je večja
- **večina organov nima možnosti celovitejše obravnave informacijske varnosti** v skladu s standardi in politikami
- **reševanje varnostnih incidentov je praviloma parcialno in nepovezano**, varnostnim grožnjam se neredko posveča premalo pozornosti
- **odsotnost sistematičnega preverjanja ranljivosti** sistemov, aplikacij, okrevalnih načrtov ipd.
- **pomanjkljivo obveščanje in ozaveščanje uporabnikov** o varnostnih grožnjah, pomanjkljivo usposabljanje IT kadrov
- **vodstva organov se večinoma zavedajo varnostnih groženj**, vendar pogosto prepuščajo vso skrb in odgovornost za informacijsko varnost zgolj IT osebju ali pa ga delegirajo na nižjo raven organizacijskih enot

Trenutno stanje v državni upravi – organiziranost IT

- **odsotnost celovite strategije** državne informatike in enotnih standardov
- **heterogenost okolij**: arhitekturna, tehnološka, procesna, organizacijska in kadrovska raznolikost organov
- **parcialne rešitve**, odsotnost skupnih gradnikov
- **razpršeni viri** (aplikacije, podatki, tehnologija)
- **podvajanje razvoja** aplikativnih rešitev, nepovezane rešitve
- **neusklajena in neracionalna poraba finančnih sredstev**, brez enotne arhitekture, strategije in ciljev.

Reorganizacija državne informatike – poglavitni ukrepi

- **oblikovanje enotne strategije** razvoja, vzdrževanja in upravljanja informacijsko komunikacijskih sistemov v državni upravi
- **uvedba enotnih tehnoloških standardov**
- **konsolidacija infrastrukture:** migracija informacijskih sistemov državne uprave v državni oblak in konsolidacija podatkovnih centrov, prenovljeno državno omrežje HKOM in širitev kapacitet, konsolidacija portfelja aplikacij
- **centralizacija nabav:** prihranki zaradi ekonomije obsega, standardizacija opreme, znižanje stroškov javnega naročanja
- **konsolidacija kadrovskih virov:** oblikovanje ustreznega strokovno usposobljenega jedra in večji obseg notranjega izvajanja storitev ter večja neodvisnost od zunanjih ponudnikov storitev
- **informacijska varnost:** enotna varnostna politika, varni sistemi, vzpostavitev Security Operational Centra, obravnavanje incidentov (SIGOV-CERT), ozaveščanje
- **vzpostavitev organizacije, ki bo enotno izvajala vse omenjene ukrepe** in dolgoročno vodila politiko razvoja, upravljanja in vzdrževanja skupnih informacijskih sistemov države, izvajala enotno varnostno politiko ter skrbela za ekonomsko najugodnejše nabave ostalih sistemov, ki ne padejo neposredno v njeno finančno okrilje.

Reorganizacija državne informatike - upravljanje

Upravljanje informacijske tehnologije bo potekalo preko štirih temeljnih stebrov:

1. **Upravljanje s podatki.**
2. **Infrastruktura.**
3. **Aplikativne rešitve.**
4. **Informacijska varnost.**

Informacijska varnost - cilji

- **Enotna ureditev** informacijske varnosti v državni upravi.
- **Prilagoditev obstoječim standardom** in izpolnitev zahtev mednarodne skupnosti, EU in NATO, po njihovem upoštevanju in ustreznem ravnanju.
- **Boljše odzivanje na varnostne incidente,** njihovo ugotavljanje in raziskovanje - vzpostavitev SIGOV-CERT, enotne kontaktne točke za odzivanje na varnostne incidente v državni upravi.
- **Zmanjšanje števila varnostnih incidentov**, ustreznejše in hitrejše ukrepanje ob njihovem pojavu.
- **Izboljšanje preventivnega odkrivanja ranljivosti v sistemih**, s tem pa povečanje varnosti delovanja informacijskih sistemov.
- **Povečanje ozaveščenosti, obveščenosti in znanja** uporabnikov informacijskih storitev ter upravljavcev informacijskih sistemov s področja informacijske varnosti.

Informacijska varnost - ukrepi

- **Priprava in uveljavitev Uredbe o informacijski varnostni politiki**.
- **Priprava in potrditev področnih varnostnih politik**.
- **Kadrovska konsolidacija** in usposobitev Sektorja za informacijsko varnost, postopoma v letih 2015, 2016 in 2017.
- **Nabava potrebne strojne in programske opreme** za izvajanje informacijske varnosti, npr. oprema za potrebe SIGOV-CERT - Security Operations Centra.
- **Izobraževanje in usposabljanje:**
  - tečaji in delavnice za informatike
  - obveščanje in opozarjanje uporabnikov
  - portal za ozaveščanje uporabnikov.

Sektor za informacijsko varnost MJU-DI (1)

Preventivno delovanje za večjo varnost informacijskih sistemov:

- normativno urejanje področja informacijske varnosti: priprava dokumentov, poročil, navodil in predpisov
- načrtovanje varnostnih zahtev in varnostnih politik
- verifikacija in implementacija varnostnih rešitev
- sistematično odkrivanje in preprečevanje ranljivosti ter varnostnih groženj v informacijskih sistemih
- varnostna analiza informacijskih sistemov (omrežja, operacijski sistemi, aplikacije, podatkovne zbirke)
- sistematično izvajanje preventivnih varnostnih preizkusov informacijskih sistemov
- priprava ukrepov za odpravo varnostnih pomanjkljivosti in izboljšanje varnosti.

Sektor za informacijsko varnost MJU-DI (2)

Obravnava varnostnih incidentov:

- vzpostavitev SIGOV-CERT za državno upravo
- sprejem in zaznava incidentov
- obravnavanje incidentov
- predlaganje in izvajanje ukrepov
- izdelava poročil.

Obveščanje, ozaveščanje in sodelovanje:

- obveščanje in ozaveščanje skrbnikov sistemov in uporabnikov v državni upravi
- izvajanje izobraževanja na področju informacijske varnosti
- sodelovanje z nacionalnimi in mednarodnimi organi ter institucijami na področju informacijske varnosti (npr. s CERT-i).
- sodelovanje na nacionalnih in mednarodnih vajah kibernetske varnosti.

Hvala za pozornost !

Damjan Križman

damjan.krizman@gov.si