dnevi slovenske informatike

"Ustvarimo nove rešitve!"

Kongresni center Grand hotel Bernardin
Portorož | Slovenija | 16. - 18. april 2012

19. konferenca
Dnevi slovenske informatike

Oblikovanje večnivojskega registra tveganj za upravljanje informacijskih in drugih tveganj

Branko Cvelbar

18. 04. 2012

slovensko društvo informatika

Oblikovanje večnivojskega registra tveganj za upravljanje informacijskih in drugih tveganj

I. Register tveganja

kot nadzorna plošča pri upravljanju tveganj

II. Informacijska varnost

v vlogi varovanja in zaščite osebnih in drugih podatkov

III. Nove rešitve: Novi poslovni model

za vzpostavljanje varnostne verige in učinkovitejše upravljanje tveganj

Oblikovanje večnivojskega registra tveganj za upravljanje informacijskih in drugih tveganj

Kriza / Tveganja / Nevarnosti / Izzivi

- Analizi stroškov birokratskih ovirah,
- Primeri (poskusov) zlorabe osebnih in drugih podatkov,
- Izkušnje z oblikovanja, nadgrajevanja in vzdrževanja državnega ERP sistema (MFERAC)

IMETI informacije / BITI informiran / SO–DELOVATI

Centralni register tveganj organizacije

CILJI in OCENA TVEGANJA					UKREPI / UPRAVLJANJE S TVEGANJI			
Zap. št. procesa	Dejavnost/CILJ, (pod)PROCES in NALOGE	TVEGANJA / opis tveganja	verjetnost (1-3) / vpliv/posledice (1-3)	S*	UKREPI	Kontrolni mehanizem	Ocena obvladovanega tveganja	S*
			VELIKA 5 / ZMERNA 4	20			SREDNJA 3 / ZMERNE 3	9

Naloge upravljanja s tveganji definiramo kot proces obvladovanja izpostavljenosti poslovanja tveganjem in omejevanja tveganj na sprejemljivi ravni. To pomeni:

- opredelitev izpostavljenosti tveganju,
- ovrednotenju ugotovljenih tveganj,
- razvrstitev po verjetnosti in teži možnih posledic.

Na podlagi takšne analize vzpostavimo primerni sistem notranjih kontrol za obvladovanje tveganj.

Register tveganj v NOE, procesih in na projektih

CILJI in OCENA TVEGANJA				UKREPI/UPRAVLJANJE S TVEGANJI			
Dejavnost/CILJ, (pod)PROCES in NALOGE	**TVEGANJA/opis tveganja**	Verjetnost (1-5) Vpliv/posledice (1-5)	S *	UKREPI	Kontrolni mehanizem	Ocena obvladovanega tveganja	
Ime procesa, cilja ali naloge, na katerega se tveganje nanaša	Kratek opis identificiranega tveganja, ki bi imel verjeten vpliv na celovitost, skladnost, zanesljivost in pravočasnost rezultatov ter izhode procesa	**Ocena verjetnosti,** da bo tveganje nastalo **Ocena vpliva** posledic tveganja na poslovanje organizacije	Zmnožek ocene verjetnosti pojava in ocene vpliva posledic, če bi tvegane razmere nastale	Seznam in kratek opis ukrepov (fizičnih, tehničnih in organizacijskih), ki bi jih morali izvesti, da bi preprečili uresničitev tveganja in ukrepov, ki bi jih izvedli v primeru, če bi se tveganje uresničilo, da zmanjšamo njegov vpliv na proces	Navede se kontrole, analize, preglede, potrdila, kazalce in drugo, kar omogoča vrednotenje upravljanja s tveganjem	**Ocena verjetnosti,** da bo tveganje nastalo, potem ko so bili izvedeni določeni ukrepe za obvladovanje tveganja **Ocena vpliva tveganja,** če bi se le-to zgodilo navkljub uresničevanju sprejetih ukrepov	Zmnožek ocene verjetnosti in ocene vpliva posledic nastanka negativnega dogodka, če bi tvegane razmere nastale navkljub temu, da smo izvedli načrtovane ukrepe za obvladovanje tveganja

naloge, procesa ali projekta

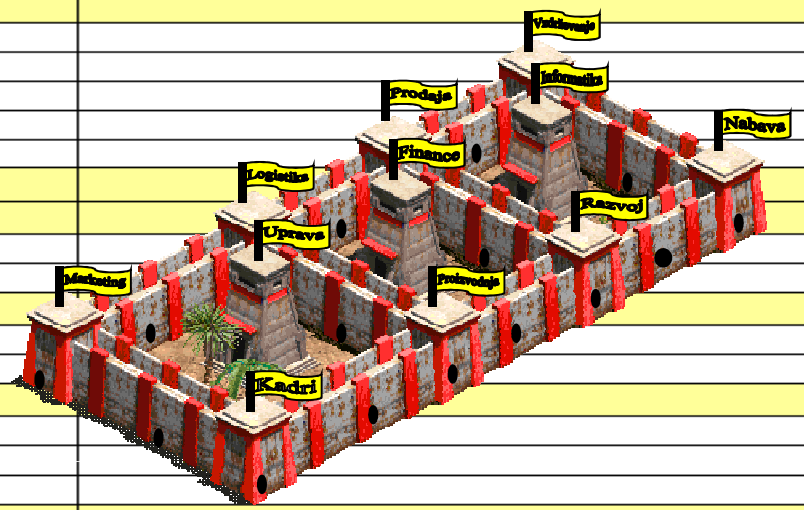
Udejanjanje upravljanja tveganj

- Upravljanje s tveganji mora biti pregleden, usklajen in splošno sprejet postopek. Pri ugotavljanju in ocenjevanju tveganj morajo sodelovati vsi zaposleni v organizaciji.
- Vodje morajo dobro poznati in razumeti svojo vlogo in odgovornosti glede tveganj. Nosilci tveganj morajo prevzeti svojo odgovornost glede tveganj in sprejemati ustrezne ukrepe.

Ne glede na to, kaj gre narobe, se bo vedno našel kdo, ki je to že vnaprej vedel.

Register tveganj informacijske varnosti 1/2

	ANALIZA ODSTOPANJ		PRIPOROČILA ZA IZBOLJŠANJE	
	Poglavja standarda ISO/IEC 27001 in ISO/IEC 27002	Ocena odstopanj	**UKREPI** HU – hitri ukrepi, PP – pomembna priporočila, OU – ostali ukrepi	Ocena izboljšanja
4	**Vzpostavitev in upravljanje varovanja informacij**			
4.1	Vzpostavitev upravljanja varnosti informacij			
4.2	Ocenjevanje informacijskih tveganj			
4.3	Upravljanje informacijskih tveganj			
4.4	Dokumentiranost upravljanja varnosti informacij			
4.5	Življenjski cikel upravljanja varnosti informacij			
5	**Varnostna politika**			
6	**Varovanje in organiziranost**			
6.1	Notranja organiziranost varovanja informacij			
6.2	Varnost v povezavi z zunanjimi izvajalci			
7	**Upravljanje sredstev**			
7.1	Odgovornost za sredstva			
7.2	Razvrščanje sredstev			
8	**Osebje in varnost**			
8.1	Pred zaposlitvijo			
8.2	Med zaposlitvijo			
8.3	Prekinitev ali zamenjava zaposlitve			
9	**Fizično in okolno varovanje**			
9.1	Varovanje prostorov in varovanje območja			
9.2	Varovanje opreme			
10	**Upravljanje obratovalnih postopkov in komunikacij**			
10.1	Odgovornost v obratovalnih postopkih			
10.2	Odgovornost zunanjih izvajalcev in dobaviteljev			
10.3	Načrtovanje in prevzemanje sistemov			
10.4	Zaščita pred zlonamerno programsko opremo			
10.5	Rezervno kopiranje			
10.6	Omrežna nadzorstva			
10.7	Rokovanje z nosilci podatkov			
10.8	Izmenjava informacij			
10.9	Elektronsko poslovanje			
10.10	Nadzor delovanja			



Analiza skladnosti s standardom ISO 27001

Register tveganj informacijske varnosti 2/2

	ANALIZA ODSTOPANJ		PRIPOROČILA ZA IZBOLJŠANJE	
	Poglavja standarda ISO/IEC 27001 in ISO/IEC 27002	Ocena odstopanj	**UKREPI** HU – hitri ukrepi, PP – pomembna priporočila, OU – ostali ukrepi	Ocena izboljšanja
11	**Ureditev dostopa do računalniške tehnologije**			
11.1	Poslovne zahteve za dostop			
11.2	Upravljanje uporabniških dostopov			
11.3	Odgovornosti uporabnikov			
11.4	Kontrola mrežnega dostopa			
11.5	Kontrola dostopa do operacijskih sistemov			
11.6	Kontrola dostopa do uporabniških rešitev in informacij			
11.7	Delo na daljavo			
12	**Nabava, razvoj in vzdrževanje sistemov**			
12.1	Varnostne zahteve v informacijskih sistemih			
12.2.	Zagotavljanje pravilnosti podatkov			
12.3	Kriptografija			
12.4	Varnost sistemskih datotek			
12.5	Varnost v razvojnih in vzdrževalnih postopkih			
13	**Upravljanje incidentov**			
13.1	Poročanje o varnostnih dogodkih in slabostih			
13.2	Upravljanje varnostnih dogodkov in izboljšave			
14	**Ureditev neprekinjenega poslovanja**			
15	**Stanje usklajenosti v zvezi z varnostjo v organizaciji**			
15.1	Skladnost z zakonodajo			
15.2	Skladnost s tehničnimi standardi			
15.3	Pregledovanje in revizija sistemov			

Analiza skladnosti s standardom ISO 27001

Učinkovitejše upravljanje informacijskih in drugih tveganj

Naše temeljno vodilo pri oblikovanju, nadgradnji … je predstavljeno v naslednji tezi:

Izkušnje in kompetence uporabnika A
+ Izkušnje in kompetence uporabnika B
+ Potrebe managementa (ključnih nosilcev odločanja)
= Garancija za sinergijo in priložnost za učinkovitejše upravljanje informacijskih in drugih tveganj,

ki nas vodi k uspešnejšemu poslovanju na poti iz kriz(e).

Pot do novih poslovnih rešitev v okviru medresorskega sodelovanja

Pogodba / Protokol / Sporazum 1/2

Primer: Osebni podatki

Osebni podatki se obdelujejo in zavarujejo v skladu s pogodbo / sporazumom, **ZVOP-1** in Pravilnikom o varovanju osebnih podatkov.

Obdelava podatkov, nadgradnja in vzdrževanje programske opreme se izvaja v lokalnem omrežju. Zagotovljeno mora biti, da:

- z oddaljenih lokacij ni možno izvajati kompleksnejših poizvedovanj,
- je oddaljen dostop realiziran preko varne povezave / navideznega zasebnega omrežja (VPN).
- prek nujnih posegov ni mogoč dostop do osebnih podatkov.
- varnostna pregrada mora imeti varnostni certifikat stopnje EAL4 ali višje,
- po večji spremembah info. sistema se izvede varnostno testiranje ranljivosti lokalnega omrežja,
- …

Pogodba / Protokol / Sporazum 2/2

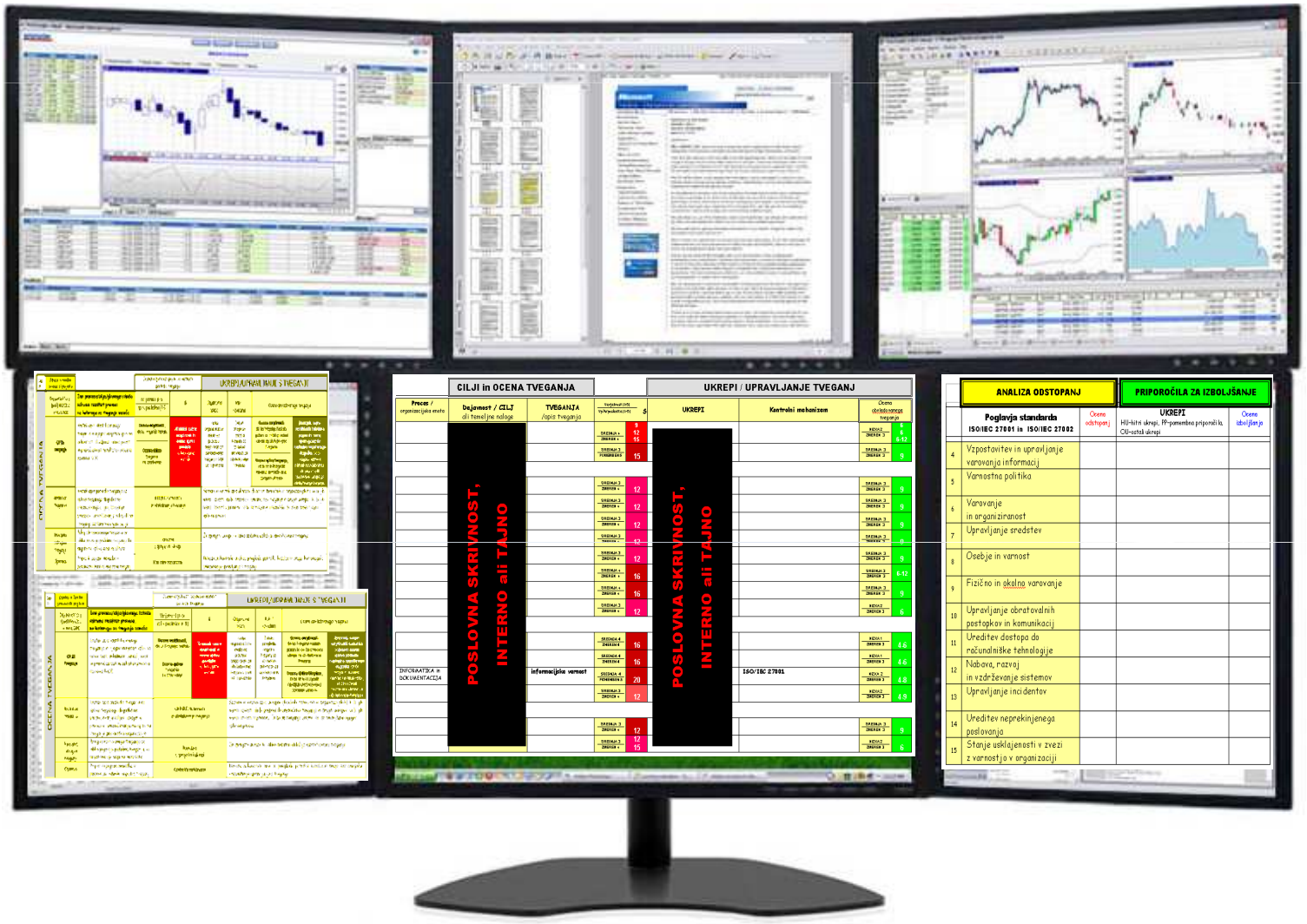
V primeru varnostnega dogodka:

- nas je pogodbenik dolžan o tem obvestiti,
- glede na oceno možnosti ogroženosti izvedemo (načrtovane)potrebne ukrepe,
- ko sami pridemo do podatkov o varnostnem dogodku, nam mora biti dana možnost vpogleda v varnostne zapise,

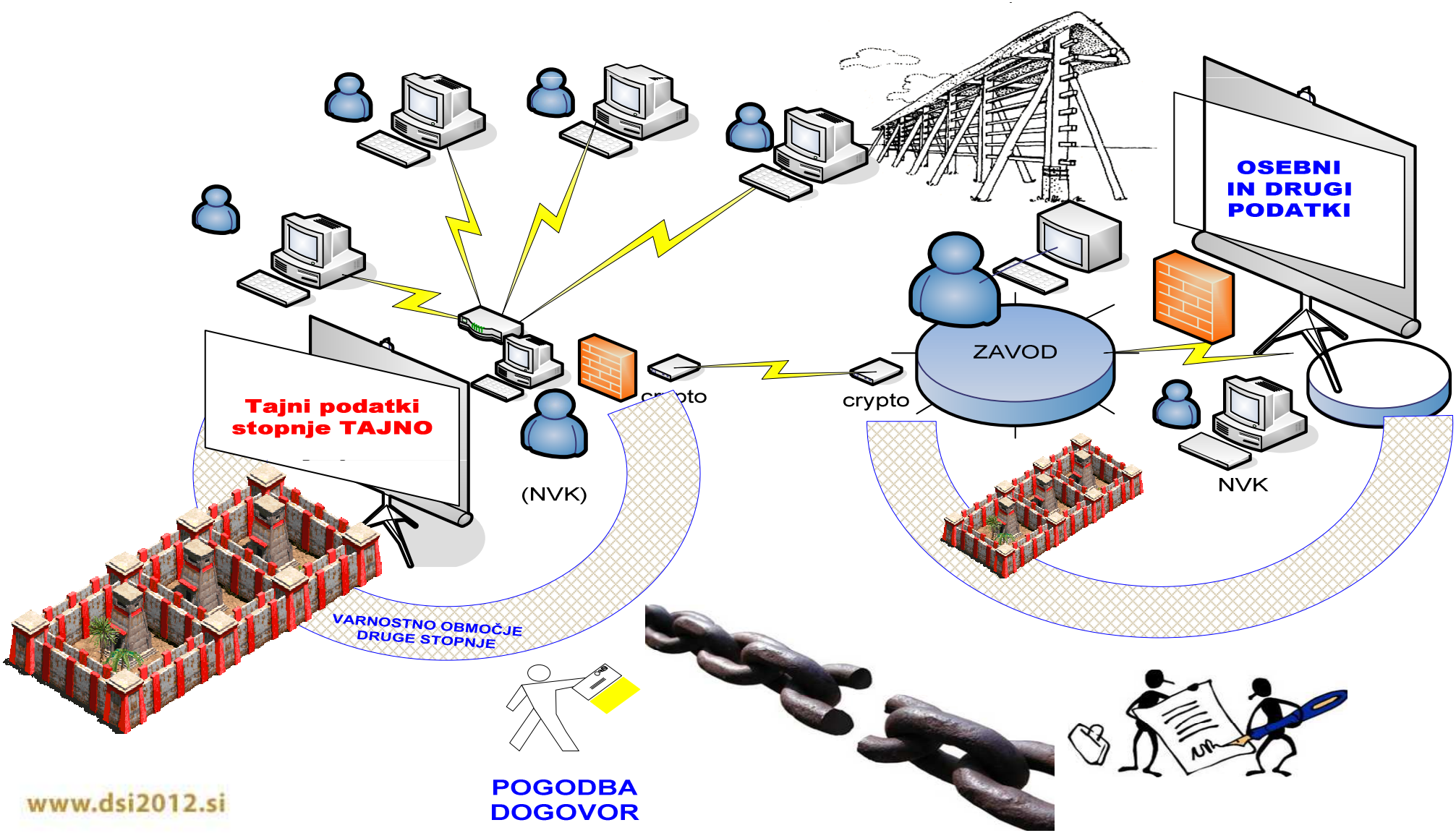
Pogodbeni partner se zavezuje:

- da bo podatke uporabljal izključno v postopkih, kot je določeno z zakonom, …
- izvedel zamejitev oziroma blokada posredovanja podatkov drugim pravnim ali fizičnim osebam.

Oblikovanje več nivojskega registra tveganj za upravljanje informacijskih in drugih tveganj



Več nivojski register tveganj in novi poslovni model upravljanja tveganj



NOVE REŠITVE
Vzpostavljanje varnostne verige in učinkovitejše upravljanje tveganj

Dobro je, da vemo,
kaj vse smo v preteklosti storili (odlično ali napak).

Pomembno je, da vemo, kaj nam je storiti,

Najpomembneje je, da imamo voljo, znanje in moč to storiti / so-delovati.

Več nivojski register tveganj in novi poslovni model kot rešitev za upravljanje informacijskih in drugih tveganj

Hvala za vašo pozornost !

brankoc@gov.si

Vprašanja?

Pripombe?

Predlogi?