Praktični vidiki vpeljave sistema upravljanja varovanja informacij (SUVI)

dr. Mina Žele
CISA
CIS-SIQ Information Security Manager/Auditor

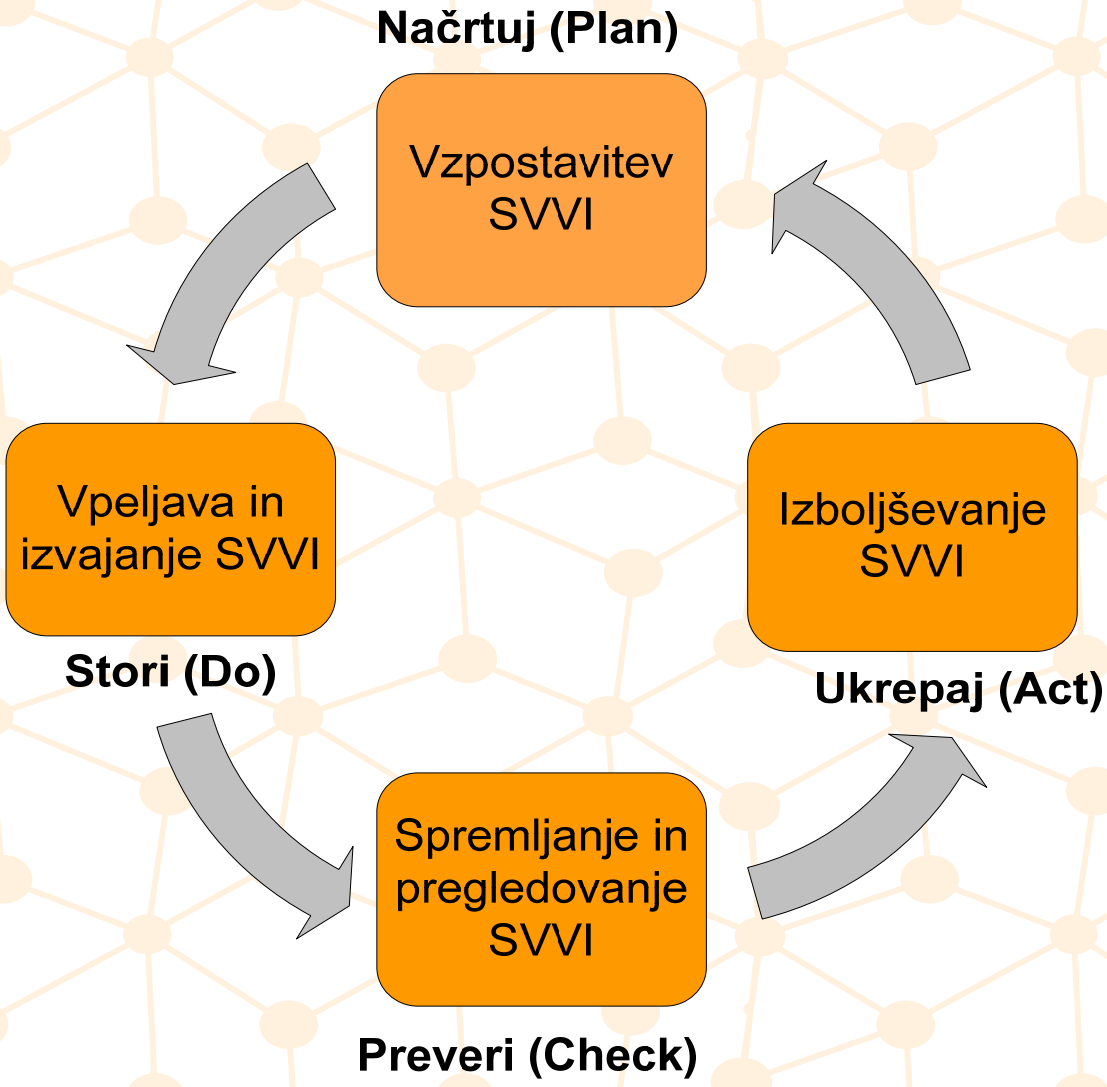
Dnevi slovenske informatike 2010

Vpeljava SUVI v organizacijo

- skladnost z zakonodajo (ZVOP, ZTP, ZVDAGA, ZEKOM)
- izboljšanje varnosti in kakovosti poslovnih procesov
- skladnost s priporočili OECD za informacijsko varnost sistemov in omrežij
- znižanje tveganja nepooblaščenega dostopa do informacij ter višji nivo varnosti informacij
- boljši nadzor tretjih strank pri zagotavljanju storitev
- povečanje razpoložljivosti in zanesljivosti storitev
- konkurenčna prednost

Sistem upravljanja varovanja informacij (SUVI)

Standard ISO/IEC 27001:2005 vsebuje zahteve za vpeljavo in vzdrževanje sistema upravljanja varovanja informacij (SUVI).



Organizacijski izzivi pri vpeljavi SUVI

Vodstvo

- Z vprašalnikom za ocenjevanje stanja in pomena informacijske varnosti se vodstvu predstavi kritičnost sistematične ureditve informacijske varnosti v organizaciji.

- Vodstvo se obvešča o vseh fazah vpeljave SUVI, izvaja nadzor in potrjuje varnostne politike, oceno tveganja in ukrepe za izboljšanje informacijske varnosti

Zaposleni

- Delavnice s področja informacijske varnosti - neprestano ozaveščanje zaposlenih o pomenu varovanja informacij in seznanjanje z varnostnimi politikami.

- Novo zaposlene se že takoj ob nastopu zaposlitve seznani z varnostnimi politikami organizacije ter pravicami in dolžnostmi v SUVI.

astec®

Organizacijski izzivi pri vpeljavi SUVI

Pravna služba

- V projekt vpeljave SUVI so vključeni že od začetka projekta in s svojim strokovnim znanjem sodelujejo pri vseh fazah vpeljave SUVI.
- Skladnost pravilnikov in internih aktov se preverja v fazi analize stanja in analize tveganja (po zahtevah ISO/IEC 27001).
- Obstoječi pravilniki se obravnavajo kot del dokumentacije SUVI tako, da se dokumenti ne podvajajo.

Odgovorna oseba za varovanje informacij

- Imenuje jo vodstvo
- Odgovorna oseba za varovanje informacij je neposredno podrejena najvišjemu vodstvu.
- Lahko je to oseba, ki je odgovorna za vodenje sistema kakovosti
- Je vezni člen med najvišjim vodstvom in ostalimi akterji na področju varovanja informacij

Naloge odgovorne osebe za varovanje informacij

- priprava dokumentov varnostne politike
- izvedba analize in obravnavanja tveganj
- zagotavljanja ozaveščenosti zaposlenih glede varovanja informacij ter ustrezne usposobljenosti
- upravljanja z varnostnimi incidenti
- izvedba varnostnih ukrepov za izboljšanje stanja varovanja informacij
- najmanj enkrat letno izvesti notranjo presojo in vodstveni pregled

Vloga analize tveganja pri vzpostavitvi optimalne varnosti

- Politike, postopke in navodila mora organizacija izdelati v skladu s svojimi spefičnimi varnostnimi zahtevami, lastnostmi okolja in procesov.
- Politike, postopki in navodila morajo biti prilagojeni na način organiziranosti, fizično okolje in že vpeljane procese in postopke v organizaciji.
- Analiza tveganja omogoči vpeljavo optimalne varnostne politike, ki odraža poslovne zahteve in je cenovno upravičena.

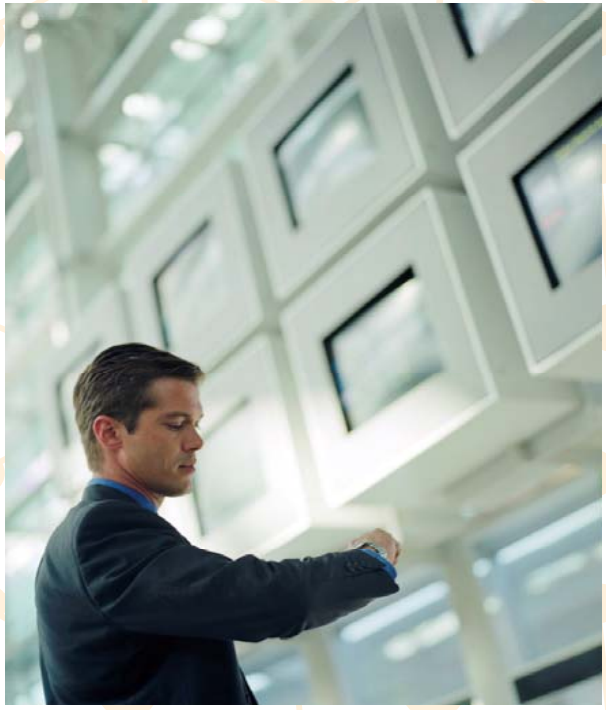
Vloga analize tveganja pri vzpostavitvi optimalne varnosti

- Z analizo tveganja ugotovimo varnostne zahteve

Kaj moramo varovati? Kakšna je vrednost informacijskih sredstev?

Kakšno je še sprejemljivo tveganje?

Kakšna je vrednost smiselnih investicij?



Katerim grožnjam so izpostavljena informacijska sredstva?

Katere so ranljivosti informacijskih sredstev?

Analiza stanja

- Zbiranje informacij- intervjuji odgovornih oseb
  - Lastniki poslovnih procesov - popis poslovnih procesov, opredelitev zahtev glede varovanja informacij, formalni in neformalni postopki na področju informacijske varnosti, popis informacijskih sredstev

  - Zaposleni v IT - trenutno uporabljene varnostne rešitve, popis informacijskih sredstev
  - Vodstvo- poslovni cilji, določitev sprejemljivega tveganja, ovrednotenje posledic groženj

Analiza tveganja

- določi prioritete za odpravo varnostnih pomanjkljivosti
- je osnova za določitev načrta izboljšanja varovanja informacij v organizaciji, saj omogoči:
  - uvedbo ustreznih tehničnih varnostnih rešitev

  - vpeljavo ustreznih postopkov, varnostnih politik in navodil

Izzivi pri izvedbi analize tveganja

- Izbira ustrezne metodologije
  - Priporočila standarda ISO/IEC 27005:2008
  - Rangiranje vhodnih podatkov (kvalitativne ocene)
  - Enostavna uporaba
  - Preglednost rezultatov
- Kako zbrati, obdelati in analizirati veliko količino podatkov
  - Uporaba namenskih programskih orodij

Avtor: racun Administratorski | Datum: 02.03.2009 | Ime: Analiza-001

Informacijska sredstva

Zap. št.	Grožnja	Ogroža	1A Informacije v elektronski obliki	1B Papirni dokumenti	1C Prenosni računalniški nosilci podatkov	1D Strežniki/oprema v sistemski sobi	1E Programska oprema	1F Prenosni računalniki	1G Delovne postaje	1H Kadri	1I Prostori	1J Infrastruktura
1. Odpoved infrastrukture												
1.1	Odpoved/okvara sredstev IT	Razpoložljivost	4 Ukrep 1.1.2		4 Ukrep 1.1.3	4 Ukrep 1.1.2		2	2			
1.2	Odpoved oskrbe z električno energijo	Razpoložljivost	5 Ukrep 1.2.1 Ukrep 1.2.2			5 Ukrep 1.2.1 Ukrep 1.2.2	5 Ukrep 1.2.1 Ukrep 1.2.2		5 Ukrep 1.2.1 Ukrep 1.2.2			5 Ukrep 1.2.1 Ukrep 1.2.2
1.3	Nihanja/sunki/udari električne energije	Razpoložljivost	3			3	3		3			3
1.4	Nezadostna zmogljivost IT/komunikacijske opreme	Razpoložljivost	2			2						2
1.5	Smrt/poškodba zaposlenih	Razpoložljivost	4 Ukrep 1.5.2			4 Ukrep 1.5.2	4 Ukrep 1.5.2			4 Ukrep 1.5.2		
1.6	Odpoved javnih komunikacij	Razpoložljivost	4 Ukrep 1.6.2 Ukrep 1.6.1 Ukrep 1.6.3									4 Ukrep 1.6.2 Ukrep 1.6.1 Ukrep 1.6.3
1.7	Odpoved/okvara komunikacijskih sistemov	Razpoložljivost	2			2	2					
1.8	Okvare merilnih naprav in sistemov	Razpoložljivost	3									
2. Zlorabe infrastrukture												
2.1	Zloraba skrbniških pravic	Razpoložljivost Celovitost Zaupnost	3			3	3		3			
2.2	Dostop tretjih oseb do sistemov/dokumentov	Razpoložljivost Celovitost Zaupnost	5 Ukrep 2.2.2 Ukrep 2.2.3 Ukrep 2.2.1 Ukrep 2.2.5	5 Ukrep 2.2.2 Ukrep 2.2.5 Ukrep 2.2.1	5 Ukrep 2.2.6	5 Ukrep 2.2.3 Ukrep 2.2.1	5 Ukrep 2.2.3 Ukrep 2.2.1	3	3			
	Socialni inženiring	Razpoložljivost										

Stanje

Nastavi zasebno
Ocena tveganja bo zasebna in vidna le lastniku oz. ustvarjalcu.

Zakleni
Ocena tveganja bo zaklenjena in jo ne bo več možno spreminjati.

Zbriši
Pobriši oceno tveganja.

Start | Administrator

ARAT- Astec Risk Assessment Tool

astec®

Tabela ukrepov

Seznam ukrepov

Zap. št.	Grožnja	Preostalo tveganje	Informacijsko sredstvo	Ukrep	Kontrole priloge A standarda ISO/IEC 27001	Stroški	Odgovorna oseba	Rok izvedbe	Datum izvedbe	Opombe	Stanje
Proces: Sprejemna pisarna											
1.1.1	1.1 Zloraba skrbniških pravic	5	Informacije v elektronski obliki Delovne postaje	Uvedba sistema za upravljanje varnostnih dogodkov in informacij SIEM	A.10.10.2 Spremljanje uporabe sistema		Žele Mina				izveden
1.4.1	1.4 Dostop tretjih oseb do sistemov/dokumentov	5	Informacije v elektronski obliki	Uvesti in dokumentirati politko prazne mize in čistega zaslona			Žele Mina		15.12.2009		izveden
1.4.2	1.4 Dostop tretjih oseb do sistemov/dokumentov	5	Informacije v elektronski obliki	Ključne aplikacije na delovnih postajah je potrebno preseliti na strežnike v sistemsko sobi, kjer je zagotovljeno ustrezno fizično varovanje. Sicer pa je potrebno delovne postaje s ključnimi aplikacijami zavarovati pred fizičnimi dostopi in izdelati načrt neprekinjenega delovanja v primeru poškodbe delovne postaje.			Žele Mina		15.12.2009		izveden
1.4.3	1.4 Dostop tretjih oseb do sistemov/dokumentov	5	Informacije v elektronski obliki	Izdelava in vpeljava politike nadzora dostopa tretjih strank v sistemsko sobo. Uvesti pravilo, da mora biti pri vstopu vzdrževalcev, osebja čistilnega servisa in obiskovalcev v sistemsko sobo prisotna pooblaščena oseba.			Žele Mina				v izvajanju
1.4.4	1.4 Dostop tretjih oseb do sistemov/dokumentov	5	Informacije v elektronski obliki	Izdelati vzorčni sporazum o varovanju informacij, ki ga morajo podpisati vse tretje stranke, ki imajo fizični ali logični dostop do sistemov, aplikacij ali informacij.			Žele Mina				v izvajanju
1.4.5	1.4 Dostop tretjih oseb do sistemov/dokumentov	5	Informacije v elektronski obliki	Prenosne medije z varnostnimi kopijami podatkov shranjevati v zaklenjeni ognjevarni omari			Žele Mina				v izvajanju
1.7.1	1.7 Zloraba uporabniških pravic	4	Informacije v elektronski obliki	Uvesti formalen postopek pregleda uporabniških pravic dostopa	A.11.2.4 Pregled uporabniških pravic do dostopa						v izvajanju
1.7.2	1.7 Zloraba uporabniških pravic	4	Informacije v elektronski obliki	Opredeliti disciplinski postopek v primeru varnostnih incidentov							v izvajanju
1.7.3	1.7 Zloraba uporabniških pravic	4	Informacije v elektronski obliki	Izvajati redna izobraževanja na področju informacijske varnosti za zaposlene						Enak ukrep kot 1.4.7	v izvajanju
Proces: Zagotavljanje delovanja IK sistema											
1.1.2	1.1 Zloraba skrbniških pravic	5	Programska oprema Strežniki Informacije v elektronski obliki	Uvedba sistema za upravljanje varnostnih dogodkov in informacij SIEM						Enak ukrep kot 1.1.1	v izvajanju
1.4.6	1.4 Dostop tretjih oseb do		Informacije v elektronski obliki	Uvesti in dokumentirati politko prazne mize in						Enak	

Varnostna politika

- Varnostna politika se mora ozirati na zakonodajo
- Standardi so primer dobre prakse
- Krovna politika je (druga) najvišja oblika predpisov, ki veljajo v organizaciji
- Področne varnostne politike (lahko po področjih standarda ISO 27002)
- S postopki in navodili zaposleni uresničujejo področne politike.
- Zadnji nivo so tehnična in izvedbena navodila

Varnostna politika

Zapisana politika mora biti dostopna, razumljiva, sprejeta in uveljavljena.

Dostopnost politike pomeni, da imajo vsi zaposleni dostop do dokumentov, da jih lahko preberejo in se strinjajo z njihovo vsebino.

Varnostne politike so jedrnate in informativne.

Novo zaposlenim se predstavi politika kot del pogojev za zaposlitev.

Vzdrževanje SUVI

- Izdelava načrta za obravnavanje tveganj - ukrepi za zmanjšanje tveganja
- Seznanitev zaposlenih z varnostno politiko
- Zaposleni in zunanje stranke, ki imajo dostop do informacij in informacijskega sistema organizacije, upoštevajo in izvajajo izdelane varnostne politike, postopke in navodila.
- Upravljanje varnostnih incidentov
- Izvajanje sestankov varnostnega foruma - usklajevanje aktivnosti za varovanje informacij med predstavniki vodstva organizacijskih enot.

p lqd}hdnC dvwhf1vl