Zasebnost

Varstvo osebnih podatkov

- V Sloveniji ureja ZVOP-1
  - Zadnje spremembe od 28.7.07, Ur.l.RS 67/2007
  - Informacijski pooblaščenec
- Inšpekcijski nadzor nad izvajanjem ZVOP-1
- Odreja ukrepe
- Vodi in vzdržuje register zbirk osebnih podatkov
- Vodi upravne postopke za izdajo ugotovitvenih odločb o tem, ali je nameravana uvedba izvajanja biometrijskih ukrepov v zasebnem sektorju v skladu z določbami ZVOP-1

Pomembnejše določbe

- Osebni podatek je v skladu s 1. tč. 6. člena ZVOP-1 katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.
- Zbirka osebnih podatkov je v skladu s 5. tč. 6. člena ZVOP-1 vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek

Katalog zbirk osebnih podatkov

- naziv zbirke
- podatke o upravljavcu
- pravno podlago za obdelavo
- vrste osebnih podatkov v zbirki
- namen obdelave
- splošen opis zavarovanja osebnih podatkov

Vsebina zavarovanja (24. člen)

- Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, **preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava** teh podatkov

Med drugim določa:

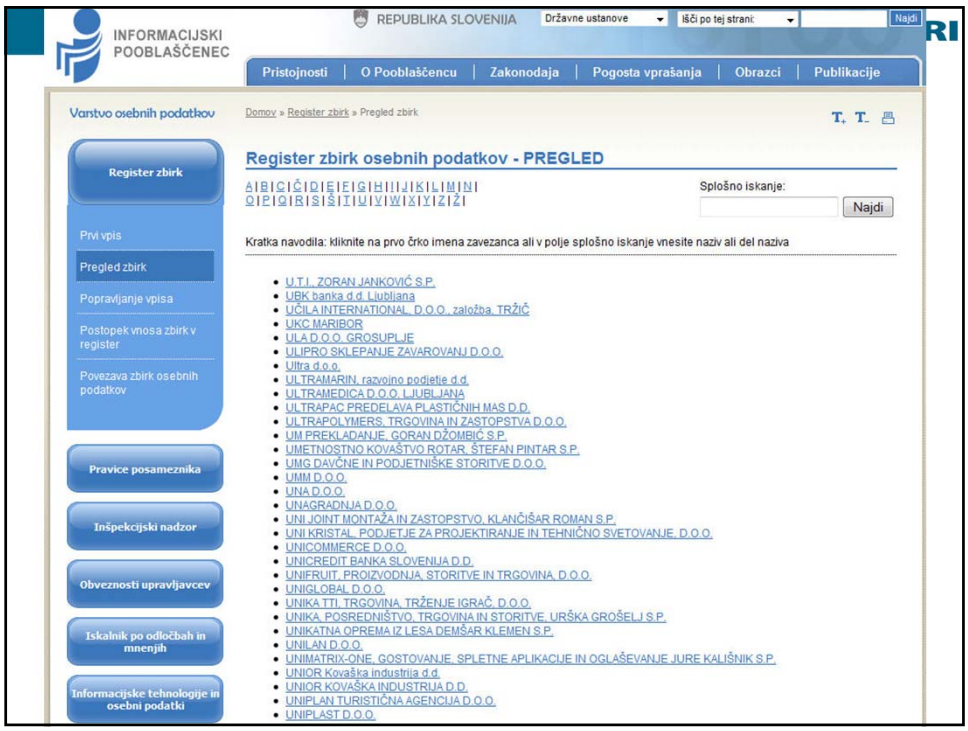
- omogoča poznejše ugotavljanje, **kdaj** so bili posamezni osebni podatki **vneseni** v zbirko osebnih podatkov, **uporabljeni** ali **drugače obdelani** in **kdo** je to storil, in sicer za obdobje, …
- postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje…

Po novem

- upravljavcem osebnih podatkov z **manj kot 50 zaposlenimi** ni treba izpolniti obveznosti iz 2. odst. 25. člena ZVOP-1 in obveznosti iz 26. in 27. člena

Informacijski pooblaščenec priporoča

- **vsaj sprejem pravilnika** iz 2. odst. 25. člena ZVOP-1, v katerem naj predpišejo postopke in ukrepe za zavarovanje osebnih podatkov
- **sprememba zakona v ničemer ne zmanjšuje obveznosti vseh upravljavcev osebnih podatkov, da te zavarujejo v skladu s 24. členom ZVOP-1**



Kako zaščiti najbolj ranljive?

- Otroki, mladostniki?
- http://www.safe.si/
- nacionalna točka osveščanja o varni rabi interneta za otroke in mladostnike v Sloveniji

Tehnično varovanje zasebnosti

Steganografija

- Skrivanje tajnih sporočil v drugih sporočilih
- Zgodovina steganografije
  - Nadomestilo za šifriranje
  - Izogibanje cenzuri
- Danes
  - Zanikanje obstoja sporočila
  - Izogibanje napadom na šifrirano sporočilo

Praktična steganografija

- Vodni žig
- Varovanje avtorskih pravic
  - Avtorska dela v elektronski obliki je "žal" možno razmnožiti z minimalnimi stroški
- Vsakdanje življenje? Posel?

Odstranjevanje skritih podatkov

- MS Word shranjuje veliko količino dodatnih podatkov o dokumentu
- Office 2003/XP Add-in: Remove Hidden Data
- http://www.microsoft.com/downloads/details.aspx?FamilyID=144e54ed-d43e-42ca-bc7b-5446d34e5360&DisplayLang=en

Obnavljanje izbrisanih podatkov

- Iz pomnilniških kartic (fotoaparati!)
  - http://www.cgsecurity.org/wiki/PhotoRec
- Iz trdih diskov
  - http://www.cgsecurity.org/wiki/TestDisk

Neposredno sporočanje brez sledi

- Izdelek VaporStream omogoča izmenjavo sporočil med dvema točkama brez sledi
  - Sporočila ni možno posredovati, shraniti, spremeniti, natisniti ali shraniti
  - Ko je prebrano, "izgine brez sledu"
  - Priloge niso dovoljene
- Način delovanja
  - Brez medpomnjenja
  - Glava sporočila in vsebina potujeta ločeno
- https://www.vaporstream.com

Ali lahko zakrijemo sledi?

- Zakrijemo izvor in prenos podatkov
  - http://tor.eff.org/
    - Ščiti uporabnika in ponudnika storitev
- Zakrijemo osebne podatke
- Spremenimo obnašanje

TOR ne zagotavlja anonimnosti

- Zaradi zagotavljanja kakovosti storitve uporablja tabelo prepustnih in zanesljivih posrednikov
- Napadalec spremeni tabelo in postane eden glavnih nosilcev prometa
- Tako lahko nadzira promet in bistveno zmanjša učinek anonimnosti

Predpisi na področju IT varnosti

Zakonska ureditev

- Zakon o elektronskem poslovanju in elektronskem podpisu (**ZEPEP)**
  - Ur.l. RS, 57/2000, 30/2001, 25/2004, 73/2004-ZN-C, 61/2006-ZEPT
- **Uredba** o pogojih za elektronsko poslovanje in elektronsko podpisovanje
  - Ur.l. RS, št. 77/2000, 2/2001, 86/2006
- Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji

Zakonska ureditev

- Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Sloveniji
  - Ur.l. RS, št. 99/2001
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Kaj je elektronski podpis

- Je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika

Varen elektronski podpis

- **Varen elektronski podpis**, overjen s **kvalificiranim potrdilom**, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.

Varen elektronski podpis

- Povezan izključno s podpisnikom
- Iz njega mogoče zanesljivo ugotoviti podpisnika
- Ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom
- Povezan s podatki, na katere se nanaša, tako da je opazna **vsaka kasnejša sprememba** teh podatkov ali povezave z njimi

Zgoščevalna funkcija (160 bit)

Kvalificirano potrdilo (certifikat)

- Je potrdilo, ki izpolnjuje zahteve iz 28. člena tega zakona in ga izda overitelj, ki deluje v skladu z zahtevami iz 29. in 36. člena tega zakona
- 28. člen
  - Navedba, da gre za kvalificirano potrdilo
  - Ime ali firma overitelja
  - Ime oz. psevdonim imetnika potrdila

Ostali predpisi

- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)
- Uredba o varstvu dokumentarnega in arhivskega gradiva
- Zakon o elektronskih komunikacijah (ZEKom)
- Zakon o varstvu osebnih podatkov (ZVOP-1)

Ostali predpisi

- Zakon o splošnem upravnem postopku (ZUP)
- Zakon o notariatu (ZN)
- Zakon o elektronskem poslovanju na trgu (ZEPT)
- Zakon o izvršbi in zavarovanju (ZIZ)
- Zakon o pravdnem postopku (ZPP)

Drugi vidiki varnosti IS

Pozorno z rabljenimi nosilci podatkov

- Izvedenih je bilo že več raziskav zbiranja in prebiranja zavrženih rabljenih nosilcev
- Dostopni so po zanemarljivih cenah ali jih lahko sami zberemo na smetišču
- Vsebujejo veliko število občutljivih podatkov
- Osebni podatki, zavarovalnine, plače, …
- Dopisi –izsiljevanje, trţni materiali, projektna dokumentacija, …

(Ne)varno indeksiranje

- Lokalni iskalniki po spletnih straneh podjetja
  - Velikokrat indeksirajo in v rezultate iskanja uvrstijo dokumente, ki so v pripravi ali sploh niso namenjeni za objavo
- Obramba
  - Pripravljanje gradiva za objavo ne spada na spletni streţnik
  - Če datoteka mora biti na spletnem streţniku potem streţniku prepovemo branje datoteke

Google kot orodje za hekerje

- Zelo učinkovit pri iskanju specifične programske opreme
- Npr. pri namestitvi Horde velikokrat administrator spregleda privzetega uporabnika “horde”
- Iskanje spletnih kamer z nespremenjenim tovarniško nastavljenim geslom ipd.

Zunanji dobavitelji in partnerji

- Winkhaus “Blue Chip” ključavnica
  - Kljub 128-bitnenm šifriranju jo lahko odpremo z malo močnejšim magnetom, s katerim premaknemo zatič ključavnice
  - Proizvajalec molči, ni obvestil strank…
- ChoicePoint
  - Masovna kraja identitete
  - Obvestili so samo tiste oškodovance, ki so jih bili po zakonu dolţni obvestiti

Varnost in gesla

Uvod

- DEFINICIJA:
  - Geslo je skrivno zaporedje (numeričnih in/ali alfanumeričnih) znakov za znanega lastnika za njegovo identifikacijo.
- CILJ:
  - Identifikacija trenutnih avtoriziranih uporabnikov, sistemov, aplikacij ali podatkov
- PROBLEMI:
  - “Ahilova peta” računalništva
  - Odgovornost uporabnika

Priporočila za oblikovanje in zavarovanje gesel

- Geslo naj bo dolgo vsaj 8 znakov
- Uporabljeni naj bodo numerični in alfanumerični znaki
- Uporabljene naj bodo velike in male črke
- Uporabljeni naj bodo posebni znaki s tipkovnice
- Združitev dveh nepovezanih besed z vezajem, rezanje nove besede na n-1 (n je predvidena dolžina besede) in vstavitev posebnega znaka s tipkovnice

Priporočila za oblikovanje in zavarovanje gesel

- Izbor tujih besed
- Uporaba zaporedja znakov s tipkovnice, ki se jih da enostavno zapomniti
- Uporaba izrazov iz dveh področij (hobi-šport) z povezavo med njima
- Gesla ne zapisujemo
- Izrazi, ki si jih enostavno zapomnimo
- Pogoste spremembe gesla

Priporočila za zaščito gesel

PRIPOROČILO
Ne zaupajte gesla NIKOMUR
Izberite geslo, ki ga je težko uganiti
Mešajte črke in številke; če je možno, tudi ostale znake in presledek Izberite pregovor in uporabite samo vsako četrto besedo; Naj računalnik izbere geslo
Ne uporabljajte gesla, ki je vaš naslov, ime hišnega ljubljenčka, ime žene/moža/prijatelja/prijateljice, ali takšno, ki je očitno (zaporedje črk ali številk)
Uporabljajte dolga gesla, šest je spodnja meja, osem je priporočljivo; daljše je geslo, težje ga je uganiti
Prepričajte se, da geslo ni vidno, ko ga vtipkujete
Prepričajte se, da geslo ni na nobenem izpisu
Ne zapisujte si gesel na mize, stene ali monitorje.
Zapomnite si gesla
Ne vključite gesla v makro ali predlogo

Priporočila za upravljanje gesel

PRIPOROČILO
Redno, vendar ne s konstantno periodo, menjajte geslo
Prikrite (kodirajte), ali kako drugače zaščitite datoteke, ki vsebujejo gesla
Dodelite administratorske pravice samo najbolj zaupanja vrednim osebam
Zamenjajte gesla uporabnikom, ki zapustijo organizacijo
Uporabniki naj za sprejeto geslo (dodeljene pravice) podpišejo izjavo
Izdelajte in zahtevajte izvajanje pravil glede gesel – in prepričajte se, da jih vsi poznajo
Ne uporabljajte skupnih gesel za vse osebe v neki domeni

Oblikovanje gesla

PRVA BESEDA	DRUGA BESEDA	POSEBEN ZNAK	GESLO
town	pick	-	pown-pi
brain	stormy	&	brain&sto
day	hot	!	hot!day
domestic	chestnut	2	dom2ches

Oblikovanje gesla

- Primer oblikovanja gesla, ki si jih lahko zapomnimo:
  - Verz iz otroštva

VERZ	GESLO
One for the money	14munny
Two for the show	24show
Three to get ready	32ready
Four to go (to)	42goto

Oblikovanje gesla

- Primer oblikovanja gesla, ki si jih lahko zapomnimo:
  - Izrazi navdihnjeni z imeni mest

MESTO	IZRAZ	GESLO
Paris	I love Paris in the springtime	ILPITST
Rome	Three(bright) coins in the Trevi fountain	TBCITTF
New York	The sidewalks of New York City	TSWONYC
San Francisco	I left my heart in San Francisco	ILMHISF

Oblikovanje gesla

- Primer oblikovanja gesla, ki si jih lahko zapomnimo:
  - Hrana, ki je v otroštvu nismo marali

HRANA	GESLO
Kikiriki oblit s čokolado	KKEKOSČ
Kokta in preste	KKTAIPR
Špinača in pire krompir	POPAJKRMP
Rižev narastek z malinovcem	RIZNMAL

Oblikovanje gesla

- Primer oblikovanja gesla, ki si jih lahko zapomnimo:
  - Transformacijske tehnike

TRANSFORMACIJA	IZRAZ	GESLO
Sprememba črk	photographic	fotografik
Prepletanje črk med več besedami	duke, iron, tent pole	diurkoen tepontle
Prevod	strangers	stranieri
Zamenjava črke z decimalnim številom	cabbage	3122175
Zamenjava decimalnega števila s črko	10.12.1492	jabadib
Prestavitev iz "začetne" pozicije na tipkovnici ob tipkanju	zucchini	uivvjomo
Substitucija sinonimov	coffe break	javarest

Oblikovanje gesla

- Primer oblikovanja gesla, ki si jih lahko zapomnimo:
  - Transformacijske tehnike

TRANSFORMACIJA	IZRAZ	GESLO
Substitucija antonimov	stoplight	startdark
Uporaba tipke SHIFT	6.6.1994	&:&:!))$
Substitucija okrajšav	relative umidity	relhum
Substitucija akronimov	Don't drink and drive association of America	DDADAOF
Ponavljanje	Pan	PanPan
Podoben izgled (180° vrtenje črk)	Swimshow	sm-wshom

Analiza razbijanja gesel

TIP GESLA	ISKALNI PROSTOR	ŠTEVILO UJEMANJ	PROCENT UJEMANJ
Ime uporabnika	130	368	2,7
Zaporedje znakov	866	22	0,2
Števila	427	9	0,1
Kitajske besede	392	56	0,4
Imena krajev	628	82	0,6
Znana imena	2239	848	4,0
Imena žensk	4280	161	1,2
Imena moških	2866	140	1,0
Nenavadna imena	4955	130	0,9

Analiza razbijanja gesel

TIP GESLA	ISKALNI PROSTOR	ŠTEVILO UJEMANJ	PROCENT UJEMANJ
Miti in legende	1246	66	0,5
Shakespeare	473	11	0,1
Športni izrazi	238	32	0,1
Znanstvena fantastika	691	59	0,4
Filmi in igralci	99	12	0,1
Risanke	92	9	0,1
Znani ljudje	290	55	0,4
Fraze	933	253	1,8
Priimki	33	9	0,1

Analiza razbijanja gesel

TIP GESLA	ISKALNI PROSTOR	ŠTEVILO UJEMANJ	PROCENT UJEMANJ
Biologija	58	1	0,0
Sistemski slovar	19683	1027	7,4
Imena strojev	9018	132	1,0
Mnemoniki	14	2	0,0
Biblija	7525	83	0,6
Razne besede	3212	54	0,4
Židovske besede	56	0	0,0
Asteroidi	2407	19	0,1
Skupaj	**62727**	**3340**	**24,2**

Navodila za uporabo gesel

FAKTOR	DEFINICIJA	MAJHNA ZAŠČITA	SREDNJA ZAŠČITA	DOBRA ZAŠČITA
Kompozicija	Nabor znakov, ki se smejo uporabljati v geslu	cifre (0..9)	črke A..Ž, črke a..ž, cifre	vsi znaki
Dolžina	Dolžina gesla (najmanjša in največja dovoljena)	4-6	4-8	6-10
Rok trajanja	Število dni veljave gesla	1 leto	6 mesecev	1 mesec
Vir	Entiteta, ki izdela geslo	uporabnik	sistem generira, uporabnik izbere	sistem
Lastnina	Kdo vse sme uporabljati geslo	uporabnik, skupina	individualna oseba	individualna oseba

Navodila za uporabo gesel

FAKTOR	DEFINICIJA	MAJHNA ZAŠČITA	SREDNJA ZAŠČITA	DOBRA ZAŠČITA
Distribucija	Kako uporabniku dodeliti geslo	navadna pošta	terminal, posebna pošta	priporočena pošta s povratnico
Hramba	Metoda hrambe gesla	v centralnem računalniku kot navaden tekst	šifriran seznam	šifriran seznam
Vnos	Način kako se geslo vnese v sistem	brez prikaza dejanskih znakov (*)	brez prikaza dejanskih znakov	brez vsakega prikaza
Prenos	Kako se geslo prenaša med vnosno in avtentifikacijsko točko	navaden tekst	navaden tekst	šifriran tekst z oznako sporočila
Perioda	Čas med dvema avtentifikacijama	za vsako transakcijo	po vsakih 10 minutah ela	po vsakih 5 minutah dela

Gesla

- Značilnosti učinkovite politike oblikovanja in uporabe gesel:
  - gesla morajo biti dovolj dolga
  - zamenjamo jih redno (npr. vsakih 60±10 dni)
  - vstavljeno geslo ne sme biti vidno na zaslonu ali papirju
  - lastniki gesel morajo biti seznanjeni z odgovornostjo in priporočili za varovanje gesel
  - zahteva se zanesljivo upravljanje gesel (varnost seznama gesel, pogosta menjava, ločitev upravljavskih funkcij gesel)
  - prikrivanje (kodiranje, šifriranje) seznamov gesel v računalniku
  - omejeno število poskusov (3 poskusi)

Gesla

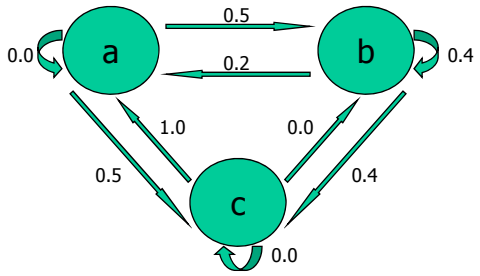
- Računalniško oblikovanje gesel:
  - naključno oblikovanje
  - možnost izbire gesla
  - težko si jih zapomnimo
  - FIPS PUB 181

Gesla

- Nadzor oblikovanja gesel:
  - proaktivni nadzornik gesel
    - uporabnik izbere geslo
    - sistem odobri ali zavrne geslo
    - uporabnik s pomočjo sistema izbere geslo, ki si ga lahko zapomni in ga je težko najti v slovarju možnih napadov
    - uravnoteženost
    - uporaba algoritmov (pravila, pregled “slabih” gesel)
  - dve tehniki oblikovanja:
    - Markov model
    - Bllomov Filter

Markov model

- M=[3, {a, b, c}, T, 1] $\Rightarrow$ [m, A, T, k]
- m=število stanj v modelu; A=prostor stanj; T=matrika verjetnosti prehodov; k=red modela (verjetnost spremembe stanja med posameznima črkama v odvisnosti od predhodne črke)
- niz, ki pripada jeziku: abbcacaba
- niz, ki ne pripada jeziku: aacccbaaa



$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$