9. POSVET DOLENJSKIH IN BELOKRANJSKIH INFORMATIKOV

INTERNETNA VARNOST

Četrtek, 24. marec 2016, ob 9.00

Konferenčna dvorana hotela Šport , Otočec

PROGRAM

8.30	**PRIHOD IN PRIJAVA UDELEŽENCEV**
9.00	**UVODNI NAGOVOR** **Dr. Mitja Cerovšek,** TPV, d. d., predsednik Sekcije za informatiko
9.05	**VARNO POSLOVANJE V KIBERNETSKEM PROSTORU** **Dr. Igor Bernik,** Fakulteta za varnostne vede in FIŠ
9.35	**S PENETRACIJO DO KANGLICE IN LOPATKE (HACK V ŽIVO)** **Grega Prešeren in Edvin Rustemagić,** S&T
10.05	**IZKUŠNJE SI-CERT NA PODROČJU KIBERNETSKE VARNOSTI** **Gorazd Božič**, SI-CERT
10.25	**ODMOR IN ČAS ZA MREŽENJE TER IZMENJAVO IDEJ**
10.55	**PREDSTAVITEV PROJEKTA APP* IN PRIKAZ AKTIVNEGA ODMORA** **Tomaž Kordiš,** GZDBK in predstavniki **Term Krka, d. o. o.**
11.05	**REFORMA EVROPSKEGA ZAKONODAJNEGA OKVIRA ZA VARSTVO OSEBNIH PODATKOV (EU DATA COMPLIANCE) IN KAKO SMO PRIPRAVLJENI** **Predrag Krstić,** Smart Data Security GmBH
11.25	**KIBERNETSKA VARNOST VIDEONADZORNIH SISTEMOV** **mag. Marko Potokar,** Inštitut za varnostno kulturo in FIŠ
11.45	**ISO 27001: MED ZAHTEVAMI STANDARDA IN PRAKSO** **Miha Ozimek**, SIQ
12.05	**KAKO SE Z INTERNETNO VARNOSTJO SOOČAJO REGIJSKA PODJETJA – PRIMERI DOBRIH PRAKS** • **Cveto Brkić,** TPV, d. d. • **Tomaž Novak,** Adria Mobil, d. o. o. • **Davor Katanović,** Krka, d. d., Novo mesto
12.50	**POVZETEK 9. POSVETA Z RAZPRAVO** **Peter Geršič,** Poesis, d. o. o., delovni predsednik posveta
13.00	**ZAKLJUČEK**

Dogodek organizira
Sekcija za informatiko v sodelovanju s
Fakulteto za informacijske študije

s&t
sponzor posveta

Vsebina

Na zagotavljanje internetne varnosti poleg ustreznih tehničnih rešitev vplivata predvsem uporabnikovo znanje ozaveščeno ravnanje. Pri obvladovanju internetne varnosti se srečujemo z različnimi varnostnimi koncepti, smernicami, politikami, orodji, zaščitnimi ukrepi in pristopi zmanjševanja tveganj. Internetna varnost je del našega poslovnega in zasebnega vsakdana, pri čemer sta razpoložljiva tehnologija in naše vedenje partnerja pri zagotavljanju varnega internetnega okolja. Varen dostop do velikih količin podatkov od kjerkoli in kadarkoli povezujemo s številnimi procesnimi, tehnološkimi, zakonskimi, socioloških in varnostnimi izzivi, ki lahko močno zaznamujejo izkušnjo internetnega uporabnika. Nahajamo se pred izzivom, kako v največji meri izkoristiti možnosti, ki jih ponuja sodobna tehnologija, hkrati pa si pri tem zagotoviti ustrezno poslovno in osebno varnost. Na posvetovanju bodo predstavljeni različni vidiki tega zanimivega področja ter konkretni primeri (dobre prakse) soočanja uspešnih podjetij z internetno varnostjo.

Vljudno vabljeni!

** Projekt APP - Atraktivna Promocija Promocije zdravja pri delu je na podlagi Javnega razpisa za sofinanciranje projektov za promocijo zdravja v letu 2015 in 2016 finančno podprl Zavod za zdravstveno zavarovanje Slovenije.*

Kotizacija
Udeležba na dogodku je za člane GZDBK brezplačna, za druge je 100 € + DDV.

Prijave na www.gzdbk.si.

Več informacij o dogodku
Andreja Vidrih, andreja.vidrih@gzdbk.si,
(07) 33 22 184

Članstvo v Sekciji za informatiko je za člane GZDBK brezplačno!

GOSPODARSKA ZBORNICA DOLENJSKE IN BELE KRAJINE

Fakulteta za informacijske študije
Faculty of information studies

9. POSVET DOLENJSKIH IN BELOKRANJSKIH INFORMATIKOV

INTERNETNA VARNOST

povzetki predavanj

Sponzor posveta

S PENETRACIJO DO KANGLICE IN LOPATKE (HACK V ŽIVO)

Grega Prešeren in Edvin Rustemagić, S&T

Na “hacku” bodo v živo predstavljene tehnike izogibanja tradicionalnim varnostnim rešitvam s posledicami izrabe. Takšne tehnike se lahko dandanes izvajajo že z odprto-kodnimi rešitvami, ki so prosto dostopne na internetu, kar pomeni, da jih lahko uspešno zlorablja praktično vsak malo bolj zainteresiran »heker« brez posebnega tehničnega znanja (npr. script kiddies). Da se ubranimo novejših vrst napadov moramo nadgraditi obstoječe varnostne rešitve z naprednimi koncepti, ki delujejo na način t.i. peskovnika.

Več na povezavi: http://www.planet.si/novice/znanost-in-tehnologija/video-zamaskirani-superjunaki-hekerji-so-povsod-vidijo-vse-tudi-nedotakljive.html

VARNO POSLOVANJE V KIBERNETSKEM PROSTORU

dr. Igor Bernik**,** Fakulteta za varnostne vede in FIŠ

Predstavljena bodo glavna izhodišča kibernetske varnosti za zagotavljanje varnega in dolgoročnega uspešnega poslovanja organizacije, razdeljena v področja obravnave informacijskega premoženja - kaj varujemo, informacijsko-varnostnih groženj - pred čem varujemo, informacijskih incidentov - kaj se lahko zgodi in ukrepov za zmanjšanje verjetnosti uresničitve groženj - da se nam ne zgodi ali ponovi.

Z zagotavljanjem glavnih področij informacijske varnosti v organizaciji namreč nadziramo glavnino tveganj, ki se pojavljajo pri poslovanju. Predstavljeni so poudarki, ki izhajajo iz poslovnih potreb in se navezujejo na uspešno poslovanje pri rabi informacijskih tehnologij in ohranjanje informacijskega premoženja. Informacijsko premoženje organizacije zagotavlja konkurenčno prednost in omogoča dolgoročno uspešnost poslovanja organizacije in ustrezno načrtovanje ter hiter odziv na spremembe na trgu. Tako bodo izpostavljena glavna izhodišča za oceno informacijskega premoženja organizacije, pregled skupin groženj, ki informacijsko premoženje ogrožajo in tveganja, ki se pojavljajo v primeru uresničitve groženj skozi informacijske incidente. Podani bodo osnovni predlogi za obravnavanje informacijskih incidentov in predstavljene zakonske podlage za zakonito obravnavo le-teh. Na podlagi omenjenega bo predstavljen model obravnavanja stroškov za zagotavljanje informacijske varnosti in obrambo pred kibernetsko kriminaliteto, ki izhaja tako iz notranjega, kot zunanjega okolja organizacije. Preko modela obravnavanja stroškov pa se seznanimo z ukrepi za ustrezno in varno poslovanje v kibernetskem prostoru.

IZKUŠNJE SI-CERT NA PODROČJU KIBERNETSKE VARNOSTI

Gorazd Božič, SI-CERT

SI-CERT je nacionalni odzivni center za omrežne incidente, ki je lani jeseni praznoval 20-letnico dela. Z informacijsko varnostjo so se torej začeli ukvarjati že zelo zgodaj, ob uvajanju interneta v Sloveniji. Obravnavajo in preiskujejo različne napade in zlorabe preko omrežja in gradijo sliko o dogajanju v slovenskem kibernetskem prostoru. Ob širših okužbah ali napadih izvajajo tudi nacionalne akcije zamejitve posledic in obveščanja skrbnikov vpletenih sistemov. Od leta 2010 izvajajo tudi nacionalni program ozaveščanja varninainternetu.si, za katerega so prejeli tudi že nekaj nagrad. V predavanju bodo predstavili trenutno stanje in nekatere zanimive omrežne incidente, ki so jih obravnavali v zadnjih nekaj letih, kaj so trenutne grožnje in kaj je potrebno storiti na nacionalnem nivoju, da se tveganja zmanjšajo. V prispevku bodo podali tudi svoj pogled na to, kaj bi morala narediti tudi podjetja sama, ne toliko pri nakupu nove opreme, ampak v spremembi pristopa in miselnosti glede informacijske varnosti.

REFORMA EVROPSKEGA ZAKONODAJNEGA OKVIRA ZA VARSTVO OSEBNIH PODATKOV (EU DATA COMPLIANCE) IN KAKO SMO PRIPRAVLJENI

Predrag Krstić, Smart Data Security GmBH

EU trenutno zaključuje novo regulativo za zaščito podatkov, ki bo predvidoma stopila v veljavo v tekočem letu. Nova regulacija nadgrajuje EU direktivo o varovanju podatkov iz leta 1995, ki zaradi globalizacije in tehnološkega napredka ne služi več prvotnemu namenu. Ena od glavnih težav obstoječe rešitve je, da gre za direktivo, kar pomeni, da je implementacije in izvajanje regulative prepuščeno posamezni državi članici EU. Neenotna ureditev predstavlja poslovnim subjektom nemalo težav. Nova regulativa prinaša višjo varnost za posameznike, poenotenje in strožjo zakonsko ureditev za organizacije.

Organizacije, ki zbirajo osebne podatke, bodo morale razmisliti o izboljšavi obstoječih in umestitvi novih procesov, ki bodo zagotavljali varnost osebnih podatkov, kot so:

1. Politika o osebnih podatkih, procedure in dokumentacija morajo biti vedno osveženi

2. Nadzorna skupina, zadolžena za pregled aktivnosti na področju osebnih podatkov. Naloga skupine je, da pripravi metriko za merjenje procesa izboljšav politike zasebnosti, in redno poroča ugotovitve.

3. Omogočiti izpolnjevanje zahteve "pravice biti pozabljen", "pravice izbrisa" in "pravice do prenosa podatkov". Priprava strategije za klasificiranje podatkov, hranjenje podatkov, zbiranje, uničevanje, shranjevanje in iskanje.

4. Implementacija procesov ob izgubi zasebnih podatkov, upravljanje teh procesov in zaznavanje izgube podatkov. Vsako izgubo podatkov je potrebno prijaviti varnostnim organom, četudi so podatki kriptirani, ali pa je možnost zlorabe nizka.

5. Priprava in uveljavljanje zasebnosti v vseh življenjskih ciklih sistema.

Kdorkoli hrani podatke o evropskih državljanih, bo podvržen novi regulativi, četudi ni prisoten v EU. V primeru izgube osebnih podatkov, je z novo regulativo zagrožena kazen do 100 milijonov € ali 5% letnega prometa. Skladnost z novo regulativo ni opcijska. Organizacije, ki so podvržene zakonom in regulacijam, morajo investirati potreben čas in energijo za zagotavljanje zakonskih obvez.

Enkripcija je najboljši način za zavarovanje podatkov.

KIBERNETSKA VARNOST VIDEONADZORNIH SISTEMOV

mag. Marko Potokar, Inštitut za varnostno kulturo in FIŠ

V današnjem času so videonadzorni sistemi ena izmed najpogosteje uporabljanih nenasilnih nadzornih tehnologij, saj je njihova uporaba nepozornim posameznikom velikokrat neopazna, kar lahko predstavlja nevarnost zlorabe. Posamezniki se obstoja video nadzora na določenem področju pogosto niti ne zavedajo oziroma se ga čez nekaj časa tako navadijo, da nanj pozabijo. Uporaba video nadzornih tehnologij je družbo razdelila na dva pola. Eni pritrjujejo mnenju, da je video nadzor učinkovit (z vidika varovanja), na drugi strani pa se civilna družba osredotoča na nevarnosti, ki izhajajo iz nadzorovanja. Tako namestitev in uporaba videonadzora po eni strani povzroča zaskrbljenost zaradi poseganja v zasebnost in strah pred kontrolo oblasti nad prebivalci, po drugi strani pa je dobrodošla, saj povečuje stopnjo varnosti in zmanjšuje družbeno nesprejemljivo vedenje.

Prvotne videonadzorne sisteme je sestavljala kamera, neposredno povezana z zaslonom, preko katerega je človek (operater) opazoval dogajanje, ki ga je prikazovala kamera. To je bila t.i. prva generacija videonadzornih sistemov z 'neumno' kamero, ki so potrebovali prisotnost človeka, ki je analiziral posnetke. Prvi generaciji videonadzornih sistemov, ki so bili analogni, je sledila druga generacija, pri kateri je bila kamera povezana z računalnikom, kar je med drugim omogočilo avtomatsko obdelavo in shranjevanje posnetkov, prepoznavo objektov in analizo okolice. Za videonadzorne sisteme druge generacije je značilna digitalizacija in digitalna obdelava podatkov. V tretjo generacijo pa sodijo videonadzorni sistemi, katerih značilnost je uporaba IP protokola in povezava v internetno omrežje.

Videonadzorni sistemi tako že dolgo niso več samo množica med seboj povezanih kamer, ki neodvisno od okolice snemajo dogajanje. Sistemi 'televizije zaprtega kroga' so tako postali informacijsko komunikacijski sistemi s svojo sistemsko in aplikativno programsko opremo ter podatkovnimi bazami, nekateri povezani v internet in temu primerno ranljivi, kot vsak drug računalniški sistem.

ISO 27001: MED ZAHTEVAMI STANDARDA IN PRAKSO

Miha Ozimek, SIQ

Razvoj informacijske tehnologije, vedno večja odvisnost od le-te, vedno večji pomen informacij so dejavniki, ki so v veliki meri pripomogli k temu, da sta nastala standarda za sisteme vodenja varovanja informacij ISO 17799 in BS 7799, danes bolj znana kot ISO/IEC 27001 in ISO/IEC 27002.

Organizacije, katerih razvoj je zahteval veliko integracijo IT rešitev v model poslovanja so se naenkrat znašle pred velikim problemom. Informacijska tehnologija je namreč zelo ranljiva, kar pomeni, da so se naenkrat močno povečala informacijska tveganja. In prav upravljanje s tveganji predstavlja eno ključnih aktivnosti v sistemu vodenja varovanja informacij (SUVI, ISMS).

Veliko organizacij se je odločilo, da bo vzpostavilo in certificiralo sistem vodenja varovanja informacij, ker je v tem sistemu prepoznalo orodje za obvladovanje informacijske varnosti. Ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij

z obvladovanjem tveganj zainteresiranim strankam vzbuja zaupanjem, da se tveganja ustrezno obvladujejo. Lahko ugotovimo, da imajo visoko tehnološko razvite države največ vpeljanih in certificiranih sistemov.

Standard ISO/IEC 27001 je zapisan v obliki zahtev, ki jih morajo v organizaciji izpolnjevati, če želijo pridobiti certifikat. Zahteve so definirane v sedmih poglavjih (4 do 10). Te zahteve morajo biti uvedene v celoti. V dodatku A pa je napisanih 114 kontrol, ki jih mora organizacija izpolnjevati. Pri tem so dovoljene opustitve, vendar mora organizacija navesti razloge za to. Kako široko obravnava standard informacijsko varnost nam kaže dejstvo, da SUVI ne obravnava samo informacijskih tehnologij in informacij v najožjem pomenu besede, temveč tudi informacije povsem organizacijske narave (klasifikacija podatkov, čista miza, fizično varovanje,…)

Izpolnjevanje zahtev standarda in s tem pravica do pridobitve certifikata se preverja na presojah, ki jih izvajajo akreditirani certiifakcijski organi. SIQ je na področju varovanja informacij vodilna certifikacijska hiša z več kot 30 podeljenimi certifikati.

Na presojah se srečujemo z različnimi rešitvami, ki so odvisne od več dejavnikov, kot so: okolje, razpoložljivi viri (človeški, finančni,..) itd. S priporočili skušamo organizacije spodbuditi k izboljšavam, ki tako ali tako predstavljajo najpomembnejši del vseh sistemov vodenja. Neskladnosti, ki jih najdemo na presojah predstavljajo priložnosti za izboljšavo in s tem zmanjšanje informacijskih tveganj.