UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

MAGISTRSKA NALOGA

JANEZ ANDERLE

KOPER, 2012

2012
MAGISTRSKA NALOGA
JANEZ ANDERLE

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MANAGEMENT

Magistrska naloga

INOVATIVNI PRISTOP PRI ZAGOTAVLJANJU VARNOSTI INFORMACIJSKIH SISTEMOV

Janez Anderle

Koper, 2012

Mentor: izr. prof. dr. Borut Likar, MBA

POVZETEK

Naloga predstavlja koncept proaktivnega pristopa varovanja informacijskega sistema (IS) in informacijskih virov, pri katerem zaposleni v organizacijah igrajo pomembno vlogo. Cilj naloge je v prvem delu predstaviti informacijske sisteme, informacijske vire in informacije organizacij. Opisane so ranljivosti in običajne tehnike njihovega varovanja. V drugem delu je prikazan proaktivni pristop k varnosti informacijskih virov in izbira ustreznih tehnik ustvarjanja idej med zaposlenimi. Podrobneje so predstavljene vse faze koncepta in pogostost izvajanja. Temeljni cilj naloge je v dveh naključno izbranih organizacijah preveriti, da je s predstavljeno metodologijo mogoče poiskati in izbrati rešitve, ki lahko prispevajo k izboljšanju varnosti obstoječega informacijskega sistema in pretoka informacij.

Ključne besede: informacijski viri, informacijska varnost, inovativni pristop, ocena tveganja, varnostni standardi.

SUMMARY

Dissertation represents the concept of a proactive approach to protect information system and information resources in which employees in enterprises and organizations, play an important role. The objective function in the first part is to represent information systems, information resources and informations of the organizations. Described are vulnerabilities and the usual techniques of their protection. The second part shows a proactive approach to security of information resources and selection of the appropriate techniques to create ideas between employees. All phases of concept and implementation frequency are presented in detail. The basic goal in two randomly selected organizations is to verify that the presented method can identify and select solutions that can contribute to improve the safety of the existing information system and information flow.

Key words: information resources, information security, innovative approach, risk assessment, security standards.

UDK: 004.056(043.2)

ZAHVALA

Najprej se želim iskreno zahvaliti svojemu mentorju, izr. prof. dr. Borutu Likarju, za ves trud, potrpežljivost in vzpodbudo med izdelavo magistrske naloge.

Ne smem pozabiti tudi rednega prof. dr. Denisa Trčka in se mu zahvaliti za vse nasvete na razgovoru ob samem začetku in za pomoč pri izdelavi dispozicije magistrske naloge, kot tudi cenjenemu zaslužnemu prof. ddr. Matjažu Muleju za posredovani kontakt v zelo uspešni gospodarski družbi, kjer sem nameraval izpeljati raziskavo. Za vse aktivnosti pri posredovanju v zvezi z raziskavo in za povabilo v laboratorij katedre se iskreno zahvaljujem prof. dr. Janezu Kopaču.

Zahvalo sem dolžan še predsedniku KSRDŠ, doc. dr. Bojanu Nastavu, da si je vzel čas za razgovor z menoj, za pojasnila, nasvete in popravke vseh nejasnosti glede vsebine in izdelave dispozicije magistrske naloge.

Posebna zahvala velja tudi moji dragi soprogi Majdi, ki me je potrpežljivo prenašala ves čas študija in me vzpodbujala, pa tudi hčerki Meti, da me je sprejela kot študenta, ki žal ni imel vedno časa zanjo.

VSEBINA

SLIKE

PREGLEDNICE

KRAJŠAVE

CAD	angl: Computer Aided Design, Programi za tehnično risanje/konstruiranje
CISCO	angl: Cisco Systems, Inc., Ameriška multinacionalna družba s sedežem v San Jose, Kalifornija
COBIT	angl: Control Objectives for Information and Related Technology, Cilji in postopki revidiranja IS
d.o.o.	družba z omejeno odgovornostjo
DRP	angl: Disaster Recovery Procedure, Postopek ponovne vzpostavitve po katastrofi
ERP	angl: Enterprise Resource Planning, Poslovni IS
EU	Evropska unija, Evropska zveza
FAQ	angl: Frequently Asked Qustions, Pogosto zastavljena vprašanja
GZS	Gospodarska zbornica Slovenije
Huawei	angl: Huawei Technologies Co. Ltd., Kitajska multinacionalna družba s področja telekomunikacijske opreme
IEEE	angl: Institute of Electrical and Electronics Engineers
ipd.	in podobno
IS	Informacijski sistem, angl: Information system
ISACA	angl: Information Systems Audit and Control Association, Organizacija revizorjev IS
ISMS	angl: Information Security Management System, Sistem za upravljanje varovanja informacij
ISO	angl: International Organization for Standardization, Mednarodna organizacija za standardizacijo
IT	Informacijska tehnologija
itd.	in tako dalje
KSF	angl: Key Success Factors, Metoda glavnih dejavnikov uspeha
LAN	angl: Local Area Network, Lokalno omrežje
MJU	Ministrstvo za javno upravo
NIST	angl: National Institute of Standards and Technology
npr.	na primer
OE	Organizacijska enota
OECD	angl: Organisation for Economic Co-operation and Development, Organizacija za gospodarsko sodelovanje in razvoj
OEM	angl: Original Equipment Manufacturer, Originalni proizvajalec opreme
oz.	oziroma
PAS 56	angl: Publicly Available Specification, Priporočila o neprekinjenem poslovanju
PDF	angl: Portable Document Format, Odprt standard za izmenjavo elektronskih dok.

PGP	angl: Pretty Good Privacy, Kriptiranje podatkov
SANS	angl: SysAdmin, Audit, Networking, and Security
SAP	nem: SAP AG, Nemški proizvajalec ERP sistemov
SVVI	Sistem za vodenje varovanja informacij
SWOT	angl: Strengths Weaknesses Opportunities Threats, Prednosti Slabosti Priložnosti Nevarnosti
t.i.	tako imenovani
tj.	to je
UPS	angl: Uninterruptable Power Supply, Neprekinjeno napajanje
WAN	angl: Wide Area Network, Prostrano komunikacijsko omrežje
Wi-Fi	angl: Wireless – Fidelity, Brezžična povezljivost
ZDA	Združene države Amerike

1 UVOD

Informacijska varnost postaja zelo pomembna za skoraj vse organizacije - ne kot osnovna dejavnost, ampak kot pomembno orodje za njeno varstvo. Iz dneva v dan smo priča novim, vse bolj ustvarjalnim metodam in sredstvom, namenjenim za krajo informacij. Bolj kot je organizacija inovativna, večji pomen ima zaščita njenenega informacijsko/inovacijskega potenciala (Likar in Trček 2012).

Da bi se učinkovito zoperstavili tovrstnim krajam, mora biti tudi zaščita informacij in virov vse bolj ustvarjalna in inovativna. V preteklosti je celo znani ekspert na tem področju prisegal predvsem na uporabo naprednih tehnologij in zapletenih matematičnih algoritmov. Svoje prvotno videnje je nadgradil s tem, ko je pomembno vlogo pri varovanju informacij pripisal ljudem oz. zaposlenim v organizaciji (Schneier 2000). Ti predstavljajo namreč nenadomestljiv prispevek na tem področju.

V pričujočem delu skušamo predstaviti metodo, ki pri zaščiti informacij in virov daje prav zaposlenim največji poudarek.

1.1 Opredelitev obravnavanega problema in teoretična izhodišča

Varovanje informacij je osnovni pogoj za tržni uspeh organizacij. Pri tem zaposleni igrajo zelo pomembno vlogo. Da so ljudje glavni dejavnik, ki ga je treba upoštevati, je ugotovil tudi ugledni strokovnjak s področja informacijske varnosti, B. Schneier, ki je sredi devetdesetih let prejšnjega stoletja prisegal predvsem na napredne tehnološke rešitve z uporabo zapletenih matematičnih algoritmov. Zaposleni namreč razpolagajo z znanjem, izkušnjami in najboljšim poznavanjem svojega delovnega okolja.

Urejene organizacije razpolagajo tudi z veliko strukturnega kapitala v obliki dokumentacije, tehničnih risb, patentov, navodil itd. Znanje je treba ustrezno zaščititi, da ne pride v roke nepooblaščenim. Enako velja za IS in ostale vire.

Za informacijsko zaščito je bila razvita vrsta standardov, med njimi družina ISO 27000 (ki se nanaša na varnostne politike), katerih pomanjkljivost so posodobitve. Te se običajno izvajajo vsakih tri do pet let. V hitro spreminjajočem se informacijskem okolju to ne zadošča več.

Alternativo kot dodatek temu predstavlja koncept proaktivnega pristopa k informacijski varnosti z vključitvijo ene od ustvarjalnih tehnik razmišljanja in s periodično uporabo v nadaljevanju predstavljene metode (Likar in Trček 2012).

Po tej metodologiji, ki je sestavljena iz petih zaporednih faz, smo se v nalogi omejili na prve tri:

- pripravljalno fazo;
- fazo iskanja in ocenjevanja varnostnih vrzeli IS;
- fazo iskanja in izbire rešitev za varnostne vrzeli IS.

Četrta in peta faza predlaganega koncepta predstavljata vpeljavo in spremljanje uvedenih predlaganih rešitev ter izvajanje ugotovljenih popravnih ukrepov. Ti dve fazi bi v nadaljevanju zahtevali opazovanje v daljšem časovnem razdobju, torej longitudinalno študijo, zato se omejimo le na prve tri.

V naši nalogi smo oceno doprinosa k informacijski varnosti, končnih izbranih rešitev za odkrite varnostne vrzeli, izvedli s polstrukturiranim intervjujem in kritično analizo. Ta vrsta intervjuja je primerna, ko gre za zaupno in komercialno občutljivo vsebino (Easterby-Smith, Thorpe in Lowe 2005, 113). Izpeljali smo jo z vodji služb za informatiko oz. predstavniki, zadolženimi za informacijsko varnost v vsaki organizaciji. V raziskavi smo predstavljeno metodologijo preverili v dveh naključno izbranih organizacijah.

1.2 Namen in cilji raziskave ter temeljna teza oz. raziskovalno vprašanje

Namen raziskave je preveriti predstavljeno metodologijo povečanja varnosti IS v praksi. Cilji raziskave so bili naslednji:

- prenos teoretičnega modela povečanja varnosti IS v prakso;
- identifikacija potencialnih varnostnih vrzeli IS v bodočnosti in določitev najbolj perečih aktualnih (sedanjih) varnostnih pomanjkljivosti, ter doseči izboljšanje informacijske varnosti v organizacijah;
- evalvacija.

Z analizo identificiranih varnostnih pomanjkljivosti IS smo skušali odgovoriti na naslednji dve raziskovalni vprašanji:

- Ali predstavljena metodologija omogoča v izbranih organizacijah poiskati varnostne vrzeli IS in rešitve zanje, ki lahko prispevajo k izboljšanju varnosti obstoječega IS in pretoka informacij?

- Ali s predstavljeno metodologijo lahko dosežemo dodano vrednost (pozitivno razliko glede na obstoječe stanje) na področju informacijske varnosti tudi v organizacijah, ki že imajo vpeljane določene varnostne politike v svoje poslovanje?

1.3 Predvidene metode raziskovanja za doseganje ciljev naloge

Za izdelavo magistrske naloge smo podrobneje preučili razpoložljiva domača in tuja znanstvena dela s področja informacijske varnosti ter ostale vire podatkov, med njimi tudi standarde, številna varnostna priporočila in dobre prakse. Metodo smo preverjali v dveh naključno izbranih organizacijah. V našem primeru gre za obravnavo širše opredeljenega problema varnosti v organizacijah. Vključena je varnost IS, virov pa tudi pomembnih strateških informacij organizacij. V okviru tega smo teoretični pristop izvedli v praksi. Ker gre za originalen pristop, ki se v podjetniški praksi ne izvaja, je bilo treba skrbno pripraviti vse faze dela. Najprej je bilo treba metodologijo in cilje ter potencialne koristi jasno predstaviti vodstvu in pridobiti njihovo soglasje za raziskavo. V nadaljevanju je sledila izbira ustreznih kadrov za sodelovanje v posameznih fazah dela glede na potrebe metodologije in kompetence sodelujočih. Za vse faze dela je bilo treba skrbno pripraviti delovna izhodišča in gradiva.

V nalogi smo se omejili na tri faze osnovne teoretične metodologije, ki predvideva pet faz. Če bi metodologijo in rešitve dejansko uporabili v organizacijah, bi varnostne rešitve spremljali v daljšem obdobju (pol leta ali dlje), kar presega okvir magistrske naloge. Tako pa smo predvidene rešitve skladno s predstavljeno metodologijo ovrednotili in ocenili, v kakšni meri bodo povečale varnost IS.

1.4 Predvidene omejitve in predpostavke pri obravnavanju problema

Predstavljena inovativna metodologija upravljanja varnosti IS in informacij ni nadomestilo za standardne metode varnosti. Gre za pristop, ki kombinirano dopolnjuje obe, standarde informacijske varnosti ter inovativno upravljanje varnosti.

V prikazu nove metodologije smo se omejili na prve tri faze novega koncepta oz. metode (pripravljalno fazo, iskanje in ocenjevanje varnostnih vrzeli IS, iskanje, usklajevanje in izbira rešitev zanje, obdelava in analiza ocenjenih predlogov vrzeli in izbranih rešitev za njihovo učinkovito odpravo). Preverjanje smo izvedli v dveh naključno izbranih organizacijah.

V organizacijah, kjer smo izpeljali raziskavo, smo se na uvodnem srečanju z vodji zaradi omejenih časovnih in kadrovskih možnosti dela s skupino dogovorili, da je ocenjevanje predlogov varnostnih vrzeli s strani izbranih ocenjevalcev potekalo posamično do dogovorjenega drugega srečanja s skupino v tretji fazi. Iz enakega razloga smo bili dogovorjeni tudi, da se je druga skupina, s katero smo iskali rešitve za ocenjene varnostne vrzeli, za končno rešitev posameznega predloga vrzeli uskladila na tem srečanju.

2 RANLJIVOSTI INFORMACIJSKEGA SISTEMA, TEHNIKE VAROVANJA IN PRIKAZ KATEGORIZACIJE INFORMACIJSKIH VIROV

Informacijski sistem (IS) je lahko katerakoli organizirana kombinacija ljudi, strojne in programske opreme, komunikacijskih omrežij in podatkovnih virov, ki zbira, preoblikuje in razširja informacije v organizaciji (O'Brien 2004, 7). Informacija je rezultat procesa interpretacije podatkov (Vidmar 2002, 25). Ti podatki imajo smisel in vrednost za prejemnika. Zaupnost, celovitost in razpoložljivost informacij so kategorije, ki lahko igrajo bistveno vlogo pri ohranjanju konkurenčne prednosti organizacije. Danes večina podatkov in informacij znotraj organizacij in z zunanjim svetom poteka v elektronski obliki medtem ko zakonodaja na številnih upravnih področjih še vedno zahteva komuniciranje tudi v papirni obliki. Pri obeh vrstah igra pomembno vlogo uporaba različnih varnostnih ukrepov. Z njimi zmanjšamo tveganje izgube podatkov oz. uhajanje informacij do nepooblaščenih znotraj ali izven organizacije na sprejemljivo raven. Vsa ta prizadevanja vplivajo na pravočasen in učinkovit odziv do priložnosti, ki se organizaciji ponudijo na trgu. Vsaka organizacija ima svoje posebne potrebe in razvito določeno kulturo. V teh okvirih si mora zasnovati profil tveganja, ki je v skladu z njeno poslovno strategijo.

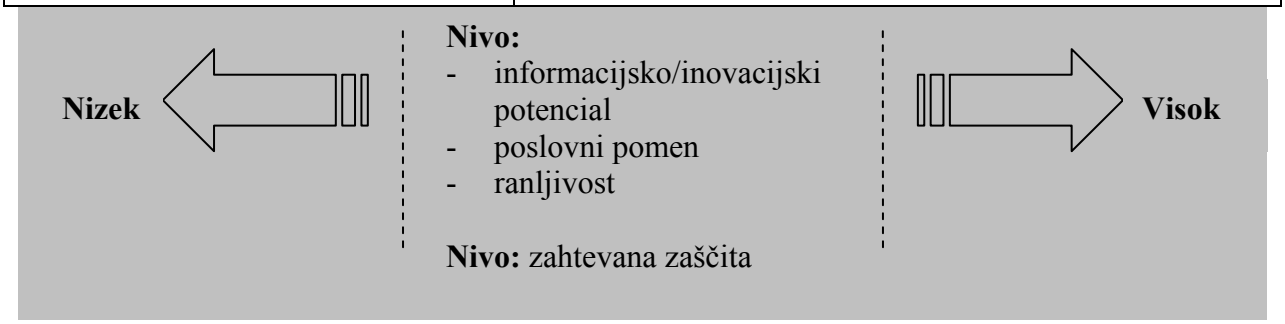
2.1 Kategorizacija informacijskih virov

V obeh naključno izbranih organizacijah, ki sta predmet raziskave, izpeljemo kategorizacijo informacijskih virov. Pri tem gre za njihovo uvrščanje po pomenu za vsak izbrani subjekt raziskave posebej.

Kategorizacijo izvedemo na enem od kratkih uvodnih razgovorov z vodji služb za informatiko ali posamezniki iz vodstva, ki problematiko področja v celoti najbolje poznajo.

V ta namen pripravimo preglednico, prikazano v prilogi 2, po vzoru slike 1, na kateri je prikazana večina najpomembnejših virov, ki naj bi jih raziskava zajela.

Skupina	Opis
Informacijski viri	Dokumentacijski podatki, podatkovne baze, elektronska sporočila, ostale datoteke, upoštevanje vseh medijev (papir, mikrofilmi, trdi disk …)
Programska oprema (angl: software)	Operacijski sistemi, uporabniška programska oprema, komunikacijska programska oprema …
Aparaturna oprema[1] (angl: hardware)	Strežniki, prenosni računalniki, stikala, tiskalniki …
Elementi infrastrukture	Klimatske naprave, sistemi za neprekinjeno napajanje …
Splošni viri	Poslovni prostori, pisarniška oprema, proizvodi in storitve organizacije …
Osebje in neopredmeteni viri	Zaposleni, poslovni partnerji, ugled pri potrošniških organizacijah, zaščitne znamke, patenti, tržni delež …



Slika 1: Kategorizacija informacijskih virov

Vir: Likar in Trček 2012.

Sogovornike v organizaciji prosimo, da izberejo pet zanje najpomembnejših virov. V prilogi 12 so povzetki, ki smo jih napravili za izbrane vire, kjer se ti pojavljajo v standardu ISO 2005b, ki pokriva večino možnih situacij. Oboje je v pomoč moderatorju seje možganske nevihte. S povzetki v obliki vprašanj si pomaga pri vodenju in usmerjanju poteka seje.

2.1.1 Informacijski viri

Informacijski viri so splošen izraz, ki vključuje vso strojno in programsko opremo, podatke in omrežja v organizaciji (Rainer, Turban in Potter 2007, 16). Vire podatkov predstavljajo tudi dokumentacijski podatki posameznih oddelkov in skupin v organizaciji oz. podatki organizacije kot celote. Dokumentacijo v elektronski obliki predstavljajo datoteke različnih formatov (pdf, doc, xls, odt, itd.), shranjene na delovnih postajah uporabnikov ali datotečnih strežnikih (npr. Novell). Podatki so lahko shranjeni tudi v strukturirani obliki ene od relacijskih baz podatkov (Oracle, DB2, MSSQL ipd.) ali elektronske pošte (Lotus Notes,

[1] Aparaturna oprema = Strojna oprema (Vidmar 2002, 75).

Outlook itd.). Vsak projekt naj bi prav tako imel dokumentirane posamezne faze dela, da se ga da uspešno voditi, nadzirati in pripeljati do želenega cilja. Dokumentacija pri tem nastaja tako v elektronski kot papirni obliki. Hranjenje določene papirne dokumentacije predpisuje tudi zakonodaja (davčni urad itd.). Vsa dokumentacija mora biti ustrezno varno shranjena, da ne pride v roke nepooblaščenim osebam, in tako, da je hitro dosegljiva za ponovno uporabo.

2.1.2 Programska oprema

V grobem lahko programsko opremo razdelimo na sistemsko in namensko uporabniško. Uporabniški program je računalniški program, namenjen podpori posebnih nalog ali poslovnih procesov (Rainer, Turban in Potter 2007, 8). Na datotečnih strežnikih in delovnih postajah je nameščena sistemska programska oprema različnih platform. Govorimo o najpogosteje uporabljenih operacijskih sistemih Unix, Linux, Novell in Windows številnih svetovnih proizvajalcev. Na izbiro sistemske programske opreme ima vpliv uporaba uporabniške programske opreme. Organizacije imajo v rabi najrazličnejšo uporabniško programsko opremo, ki je večinoma odvisna od dejavnosti, katero opravljajo. Proizvodne organizacije imajo v uporabi različne ERP sisteme, ki z več moduli pokrivajo celotni proizvodni proces (nabava, proizvodnja, prodaja, finance, servis). Med programsko opremo štejemo še različne računalniške rešitve za obvladovanje elektronske pošte, razvojno načrtovanje in planiranje (CAD), dokumentne sisteme itd. Obstaja še cela vrsta komunikacijske programske opreme za zagotavljanje in nadzor komunikacijskih povezav itn. Veliko uporabniške programske opreme se izvaja tudi preko spletnih tehnologij (spletne rešitve, računalništvo v oblaku itd).

2.1.3 Aparaturna oprema in elementi infrastrukture

V večini organizacij ali ustanov je za namestitev vitalnih delov strojne opreme namenjen poseben prostor, t. i. sistemski prostor, ki je klimatiziran. Vanj naj bi imele dostop le pooblaščene osebe iz oddelka informatike. V sistemskem prostoru so nameščene različne vrste strežnikov (datotečni, podatkovni, poštni, spletni itd.), usmerjevalnikov za pravilno in optimalno usmerjanje podatkov po različnih mrežnih segmentih, požarnih zidov in stikal (angl: switch), ki omogočajo priključevanje delovnih postaj in strežnikov v zaključeni IS. Za primere izpada električne napetosti so v sistemskem prostoru nameščene naprave za neprekinjeno napajanje (UPS). To so baterije, ki s pomočjo inteligentne elektronike v primeru električnih izpadov varno izključijo strežnike. V nasprotnem primeru bi prišlo zaradi prehodnega pojava izpada napetosti do nepredvidljivih napak na podatkih ali strežniški opremi (diskovnih enotah, napajalnikih ipd.). Med strojno opremo štejemo še prenosne in tablične računalnike, večfunkcijske naprave, ki združujejo kopirni stroj, optični čitalnik, faks in tiskalnik v eni sami enoti. Sledijo tiskalniki za centralno izpisovanje podatkov (angl: line printers), risalniki (angl: ploterji) itd.

2.1.4 Splošni viri

Med splošne vire uvrščamo poslovne prostore, pisarniško opremo ter proizvode in storitve organizacije. Poslovni prostori so namenjeni zaposlenim za opravljanje njihove dejavnosti. V njih morajo biti zunanji obiskovalci vedno v spremstvu in pod nadzorom zaposlenih.

2.1.5 Osebje in neopredmeteni viri

Zaposleni v organizacijah razpolagajo z mnogimi znanji in informacijami, ki so lahko povezane z njihovim delovnim mestom, pa tudi s širšim poznavanjem problematike organizacije. Ta znanja in informacije naj ne bi prišle do nepooblaščenih oseb ali konkurence. Veliko informacij o organizaciji imajo tudi poslovni partnerji, ki z njo kakorkoli sodelujejo. Da se zavedajo odgovornosti do njenih podatkov in informacij, mora biti sporočilo varnostne politike organizacije jasno zapisano v pogodbi o medsebojnem sodelovanju (Peltier 2005, 39). Poleg naštetih je v poslovnih in ostalih subjektih še cela vrsta neopredmetenih virov. Predstavljajo jih blagovne znamke, različni postopki, recepture, tržni deleži, ugled organizacije pri kupcih itd. Gre za zelo pomembno kategorijo virov, še posebej med njimi so to na trgu uveljavljene blagovne znamke, od katerih je lahko odvisen celo obstoj organizacije.

2.2 Ranljivost IS

Ranljivost predstavlja slabost vira ali skupine virov, ki jo lahko izrabi ena ali več groženj (ISO 2005b, 3). Informacije predstavljajo za ozaveščeno organizacijo premoženje. Zaposleni se morajo zavedati, da je informacija pomemben vir organizacije, ki predstavlja njeno lastnino (Peltier 2005, 49). Če zaposleni niso dovolj dobro seznanjeni z zaupnostjo informacije oz. njeno zaščito, odgovorno osebje ne le da tvega zlorabo enega najpomembnejših virov organizacije, temveč tvega tudi neskladje z vse večjim številom zakonov in regulativ s tega področja (Herold 2010). Ogrožen je lahko tudi ugled organizacije. Brez dobrega ugleda pa začne organizacija izgubljati stranke, čemur sledi upad prodaje in s tem dohodka. V ZDA, na primer, zakonodaja organizacijam, ki poslujejo javno, predpisuje oceno učinkovitosti svojih internih varnostnih kontrol, pri čemer morajo zagotoviti neodvisne nadzornike, ki na koncu potrdijo veljavnost ocen poročil, varovanja zasebnosti in izobraževanja zaposlenih v organizaciji (Sarbanes-Oxley Act 2002).

Organizacije, ki tržijo svoje strežniške kapacitete in uporabniško programsko opremo, kot npr. izračun plač, operirajo z veliko količino zaupnih podatkov in informacij. Vse te podatke so dolžna varovati že po Zakonu o varstvu osebnih podatkov (ZVOP-1-UPB1), da ne pridejo preko njihovega IS ali zaposlenih v roke nepooblaščenim. V naši državi je za nadzor nad izvajanjem zakona o varstvu osebnih podatkov pristojen informacijski pooblaščenec. Gre za prekrškovni organ, ki ima pristojnost tudi za nadzor Zakona o Informacijskem pooblaščencu (ZInfP).

Številne, tudi naše, organizacije nudijo strankam varnostno preverjanje ranljivosti njihovega IS. To izpeljejo z ustreznimi postopki preverjanja, ko nadzorovano in dokumentirano simulirajo poskus vdora v IS stranke s strani enega ali več "napadalcev". Izvajalec preverjanja

ima v skladu z dogovorom s stranko na voljo vse informacije, ki so dostopne drugim zaposlenim. Gre za simulacijo delnega poznavanja omrežja, kakršnega ima npr. "zlonamerni zaposleni", ki predstavlja enega najpogostejših vzrokov varnostnih incidentov v organizacijah (Smart Com d.o.o. 2012).

Prava informacija ob pravem času in na pravem mestu lahko predstavlja konkurenčno prednost. Teoretično je ranljiv vsak vzpostavljen IS s katerim obvladujemo elektronske vire informacij.

2.2.1 Varnostni incidenti

Varnostni incident predstavlja uresničeno grožnjo. Neodvisne raziskave so pokazale, da se le dve tretjini organizacij po svetu zaveda nevarnosti, ki jo prinašata elektronsko poslovanje in uporaba interneta. Od tega jih samo ena tretjina intenzivno dela na učinkovitem izvajanju informacijske varnosti. Razloge za to gre iskati predvsem v napačnem razumevanju področja informacijske varnosti s strani vodstva in popolnega ignoriranja posledic, ki bi lahko nastale ob nastopu informacijske nesreče. Nesprejeta ustrezna varnostna politika je lahko vzrok spletne goljufije. Zato mora organizacija skrbno analizirati svoje procese in poskusiti najti katerokoli še nepoznano tveganje, ki obstaja. Dogaja se, da so v organizacijah podatki, shranjeni na računalnikih, še sorazmerno dobro zaščiteni. Slabše je po navadi s podatki, ki so shranjeni v papirni obliki. Tovrstno hrambo namreč še vedno zahteva zakonodaja. Organizacija brez zaščitene papirne dokumentacije je skoraj kot organizacija brez informacijske zaščite. Nujno je treba ločiti dnevno papirno dokumentacijo od tiste, ki mora biti shranjena v protipožarnem sefu (InfoSecurityLab 2012).

Metodologije, razvite za učinkovit odgovor na incidente, dajejo velik poudarek sami pripravi. Še posebej, da se organizacija pripravi za učinkovit odgovor nanje v preventivnem smislu tako, da so njeni sistemi, omrežja in računalniške rešitve dovolj varni. Ker obstaja nešteto načinov, da se incident zgodi, ni praktično pripravljati postopkov za vsakega posebej. Bistvene faze odgovora na incidente pa so: začetna priprava, odkrivanje in analiza, ustrezne akcije za zmanjšanje posledic, odpravo in "okrevanje" ter ukrepi po incidentu (NIST 2008, 3-1).

2.2.2 Varnostne grožnje

Informacijski viri, ki sestavljajo posamezne temeljne poslovne procese, so izpostavljeni tveganjem glede zaupnosti, celovitosti ter razpoložljivosti. To so tri glavne lastnosti, ki predstavljajo vrednost informacije (ISO 2005a, 2-3). Ločimo aktivne in pasivne poslovne grožnje. Aktivne povzročajo vdiralci v sisteme s pisanjem in razdeljevanjem programskih in makro virusov, trojanskih konjev ter črvov, konkurenca organizacije pa tudi nezadovoljni zaposleni znotraj nje. Nezadovoljni ali nepošteni zaposleni so stalna grožnja in neprevidnost ima lahko hude posledice. Še zlasti jo lahko izkoristijo nepridipravi s prenosnimi računalniki

in dlančniki. Osebja na visokih položajih in skrbnikov s praktično neomejenimi pooblastili za dostop skoraj ni mogoče zaustaviti (Greengard 2011).

Pri iskanju varnostnih groženj, ki jih lahko povzroči človek, moramo imeti v mislih možne motive, ki človeka privedejo do dejanja, in metodo, s katero se ga bo lotil. Pri iskanju potencialnih storilcev so nam lahko v oporo pregledi arhiva podobnih situacij v organizaciji, poročila kršenja varnostne politike, zabeležke incidentov, razgovor s sistemskim administratorjem ali osebjem, ki skrbi za pomoč uporabnikom (NIST 2002, 13). Dodatna skrb so tudi dostavno osebje, začasni delavci in celo vratarji, ki jim je pogosto dovoljeno nemoteno gibanje po prostorih organizacije.

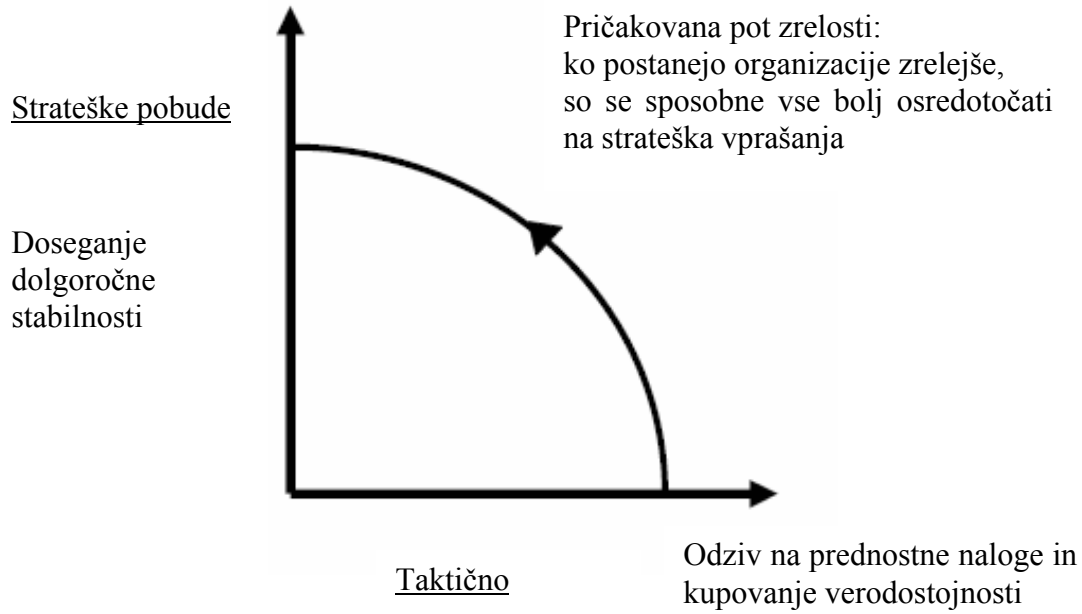
Podatkom in informacijam pretijo še pasivne grožnje, med katere med ostalimi štejemo naravne nesreče na potresnem, vetrovnem ali poplavnem območje organizacije, okvare strojne in programske opreme, človeške napake ter komunikacijske in energetske prekinitve. Informacijsko varnost ogrožajo tudi nezavarovane brezžične dostopne točke do omrežja, zlorabe socialnih omrežij itd.

Zakonodaja še vedno zahteva hranjenje velikega števila podatkov v fizični, papirni obliki. Veliko grožnjo pri tem predstavlja požar, zato moramo te podatke hraniti v požarno varnih omarah. Enako velja za podatke zaščitnih kopij IS (backup). Da zmanjšamo možnost izgube podatkov, je zaželeno, da so ti hranjeni vsaj na dveh fizično ločenih lokacijah.

Novosti v zakonodaji tega področja naj bi do določene mere ščitile organizacije. Sprejeta je običajno veliko počasneje, kot pa si sledijo incidenti informacijske varnosti, s katerimi se soočajo. Na področju mrežnih in internetnih tehnologij je bil storjen izredno velik napredek. Za povezavo med organizacijami danes internet predstavlja nov poslovni model. Kot medij pa je žal tudi izredno odprt. S seboj je zato prinesel veliko novih izzivov na področju varovanja informacij.

Tveganje na področju informacijske varnosti se je močno povečalo. Zato je potreben proaktiven pristop do njegovega upravljanja, če se želi izkoristiti vse tehnološke prednosti, ki so na voljo. Že v zgodnji fazi priprave neke realistične strategije informacijske varnosti je treba upoštevati, kako "zrel" je trenutni pristop do tega vprašanja. Iz tega se naprej da ugotoviti, koliko in katere aktivnosti je treba izvesti bolj v taktičnem in koliko v strateškem smislu.

Na splošno velja, kot je razvidno na sliki 2, da morajo mlajše in manj izkušene organizacije napraviti več v taktičnem smislu, medtem ko so bolj izkušene in uveljavljene že sposobne več časa nameniti strateškemu področju.



Slika 2: Prehod iz taktičnega v strateško področje glede na zrelost organizacije

Vir: Purser 2004b.

Razvijalci varnostnih modulov operacijskega sistema se srečujejo s problemom, da so ti po navadi zelo obsežni in zato še polni programerskih napak. Sisteme, ki gredo v produkcijo, nato preverja veliko število uporabnikov po svetu hkrati. Dogaja se, da kdo med njimi po naključju odkrije napako in je ne sporoči razvijalcem oz. proizvajalcu, temveč informacijo o napaki objavi na spletnem forumu (Anderson 2001, 68). Zakasnitve od trenutka, ko se objavi določena ranljivost, pa do trenutka, ko hekerji z napadi takšno ranljivost izkoristijo, se hitro zmanjšujejo. Zato so se organizacije v času, dokler proizvajalci programske opreme in protivirusnih programov ne zagotovijo ustreznih popravkov, prisiljene zaščititi same (Purser 2004b).

Ranljivost je vsaka pomanjkljivost IS in dobrin, ki jo lahko določena grožnja izrabi. Stopnja ranljivosti IS je odvisna od učinkovitosti že uvedenih ukrepov varovanja.

Šibke točke oz. ranljivosti v IS se lahko namerno izkoristi z vnosom najrazličnejših računalniških virusov za prisluškovanje na omrežju ali delovnih postajah itd. Grožnjo kot posledico zaradi ranljivih delov sistema lahko sproži tudi zaposleni z nenamernim ali nepremišljenim dejanjem. Preprosta konfiguracijska napaka IT strokovnjaka lahko pusti odprta mrežna vrata, ranljiv požarni zid (firewall) ali popolnoma nezaščitene sisteme. Omenjeni požarni zid predstavlja skupino naprav z namensko programsko opremo, ki varno povezuje "zaupno notranje omrežje" z zunanjim, javnim omrežjem. Paketi podatkov, ki preko njega potekajo, morajo biti preverjeni z nizom pravil, določenih v varnostni politiki, da jih

avtorizirajo in spuščajo skozi (Stefanek 2002, 23). Hinson (2003, 3) trdi: "Človeška napaka veliko bolj verjetno povzroči resne kršitve varnosti kot morebitne tehnične ranljivosti."

Informacija v elektronski obliki potuje skozi več ciklov. Na začetku gre za zasnovo ali generacijo informacije, ki se jo nekje shrani. V tej obliki je nato na voljo za uporabo. Obdelava z drugimi informacijami da z njo nov rezultat, ki se kot tak prenese na naslednje mesto, to je lahko k naročniku te informacije ali pa ta informacija služi v organizaciji za vrednotenje nekega postopka, procesa itd. Informaciji je običajno treba določiti tudi čas njene hrambe. Po preteku tega dogovora se določi način bodisi za arhiviranje informacije ali njeno uničenje. Z uničenjem se cikel informacije zaključi.

Posledica vedno večje medsebojne povezanosti IS in omrežij je, da so ti izpostavljeni različnim vrstam groženj in ranljivostim. To zahteva stalno izboljšavo varnostnih rešitev in potrebo po vse večji ozaveščenosti ter razumevanju varnostnih vprašanj kot tudi razvoju varnostne kulture (OECD 2002). V zadnjem obdobju pomeni velik premik na področju informacijske varnosti že spoznanje, da je varnost predvsem tudi poslovno vprašanje. Pri razvoju varnostne kulture organizacije igra odločilno vlogo zavedanje vodstva o teh vprašanjih in izobraževanje zaposlenih. Le ozaveščeni uporabniki bodo znali ceniti prizadevanje vodstva, da preko svojih pooblaščencev v IT službi preprečuje širjenje virusov in zlonamerne kode preko sporočil elektronske pošte ipd. Samo vprašanje časa namreč je, da se okužba z delovne postaje uporabnika prenese na strežnik. Slabo razvite in prilagojene kulturne vrednote na področju sistemske administracije imajo lahko resne varnostne posledice na strežniški strani (primeri nedosledne in sprotne analize log datotek[2] produkcijskega sistema itd.). Upravljanje z log datotekami je v korist organizaciji na več načinov. Z njim zagotovimo, da so podrobni varnostni zapisi sistema ustrezno dolgo shranjeni. To pomaga odkrivati in prepoznati varnostne incidente, kršitve varnostne politike, goljufije, izvajati forenzične analize itd. (NIST 2006, 2-7). V takih in podobnih organizacijah zahteva vpeljava sprememb obstoječe kulture, združitev številnih varnostnih konceptov v novo delovno kulturo. Obstaja veliko literature in dokumentacije o formalnih metodah, katerih poudarek je na vključitvi področja informacijske varnosti, v kulturo organizacije (Purser 2004a).

2.2.3 Fluktuacija in migracije zaposlenih

Organizacije, v katerih se delovna sila menja hitreje, bodisi zaradi težjih pogojev, narave dela ali boljših plač konkurence, se morajo še posebej zavedati zaščite svojih podatkov in informacij. Uhajanju poslovnih informacij h konkurenci se lahko izognejo z ustrezno pogodbo o zaposlitvi, pogodbo o varovanju poslovnih skrivnosti oz. konkurenčno klavzulo. V primeru kršitve določil ene od teh pogodb lahko zaposleni ali pogodbeni partner odškodninsko odgovarja za ocenjeno nastalo škodo oz. za znesek, ki je naveden v taki pogodbi. V isti okvir je treba šteti tudi zelo razširjeno študentsko ali sezonsko delo. Sem spada opravljanje obvezne prakse, pripravništvo in pa vajeništvo. Naslednjo pomembno kategorijo predstavljajo nezadovoljni zaposleni ali zaposleni, ki so si službo našli v drugi organizaciji. Ti so kot

[2] Operacijski sistemi in uporabniški programi v teh datotekah beležijo sledi interno izvedenih akcij.

"napadalci" najbolj nevarni, saj natančno vedo, katere informacije iščejo, kje jih bodo našli in kako se lahko do njih dokopljejo. Zelo pomembno je, da skrbnik IS takoj odvzame vsa pooblastila in dostope zaposlenim, ki so prenehali z delovnim razmerjem. Vodstvo organizacije lahko sprejme tudi sklep, da se odvzame ali omeji pooblastila na IS tudi odhajajočemu zaposlenemu še v času dogovorjenega ali zakonitega odpovednega roka. To velja posebej, če gre za odpoved delovnega razmerja iz krivdnih razlogov s strani delodajalca.

2.2.4 Odtujitve informacijskih virov, podatkov in informacij

V današnjem dinamičnem poslovnem okolju predstavlja zahteva po mobilnosti potencialno nevarnost kraje sodobnih prenosnih komunikacijskih naprav. Mednje ne sodijo le klasični prenosni računalniki, temveč tudi vse bolj zmogljivi mobilni telefoni in tablični računalniki. Pri tem tvegamo izgubo občutljivih podatkov na napravah, kot so naši osebni podatki, podatki o zaposlenih in poslovnih partnerjih, osnutki različnih pogodb, cenikov, projektov itd. Deloma se proti kraji lahko zaščitimo s šifriranjem podatkov. S tem jih napravimo neuporabne za vse tiste, ki ne poznajo šifrirnega ključa.

Prenosniki in tablice omogočajo tudi brezžični Wi-Fi dostop do svetovnega spleta. Brezplačna javna brezžična omrežja so nam na voljo na številnih mestih (hoteli, knjižnice, internetne kavarne itd.). Večina jih je nešifriranih in torej nezaščitenih. To pomeni, da je mogoče podatke, ki potujejo med našo napravo in brezžičnim usmerjevalnikom, prestreči s strani tretjih oseb, ki so morda v bližini brezžičnega omrežja. Še preprostejši način dostopa do informacij pa predstavlja pogovor s poslovnimi partnerji ali znanci na javnih mestih. Pomembni poslovni pogovori se zato vodijo izključno na mestih, ki omogočajo diskretnost, brez možnosti, da pogovor "ujame" tretja oseba.

2.3 Prikaz običajnih načinov in tehnik varovanja IS v organizacijah

Dokler organizacije ne pristopijo k celovitemu sistemu upravljanja informacij ISMS, po navadi pri njih prevladujejo posamične in ne združene varnostne kontrole. Prve nastajajo spontano kot posledica zadostitve specifičnih varnostnih situacij ali kot zaveza kakšnega novega sporazuma, uredbe ipd. V organizacijah obstajajo, ali pa tudi ne, različni interni pravilniki in varnostne politike, ki po navadi pokrivajo le del obravnavanega področja. Leta 2010 so bila, za primer, na področju delovanja javne uprave, sprejeta priporočila informacijske varnostne politike z namenom, da se zaščiti informacijsko premoženje, ki ga upravlja (MJU 2010). V organizaciji, ki smo jo zajeli v naši raziskavi, so imeli nedavno v veljavi interni predpis o informacijski varnosti. Iz njega je jasno razbrati zavedanje odgovornih o tem, da so informacije del premoženja organizacije, ki jih je, prav tako kot ostale vire, treba zaščititi. Svoj varnostni koncept nameravajo še nadgradili. Pri tem jim bodo v pomoč tudi rezultati naše raziskave. Pred osmimi leti je Inštitut za informacijsko varnost izdelal prvo resno raziskavo o informacijski varnosti pri nas. Cilj raziskave je bil oceniti stanje na področju informacijske varnosti v slovenskih organizacijah. Raziskava je bila izvedena s pomočjo telefona kot tudi s pomočjo daljše pisne ankete. Na vprašanje, če imajo

organizacije formalno definirano in napisano varnostno politiko, se jih je takrat približno petdeset odstotkov izreklo pozitivno (Židanik et al. 2004). Razveseljivo je dejstvo, da se stanje na tem področju dandanes izboljšuje. Poleg bank, zavarovalnic, organizacij s področja telekomunikacij in podobnih institucij se za pridobitev certifikata s področja varovanja informacij, ISO 27001, odloča vse več tistih organizacij, ki imajo dnevno opravka z veliko količino osebnih podatkov. Organizacije se zavedajo, da se s tem dvigne tudi njihova bonitetna ocena. Tako laže konkurirajo na domačih in mednarodnih razpisih za različne projekte.

Odstavek 404 SOX[3] od organizacij v ZDA, ki poslujejo javno, zahteva, da ocenijo učinkovitost svojih internih kontrol za finančni nadzor, ki zagotavljajo letna poročila za vsako fiskalno leto. Glavni informacijski nadzorniki so zadolženi za varnost, natančnost in zanesljivost sistemov, ki obvladujejo in poročajo finančne podatke. Zakon od organizacij, ki poslujejo javno, zahteva tudi, da zagotovijo neodvisne nadzornike, ki morajo potrditi veljavnost ocen končnega poročila (Sarbanes-Oxley Act 2002).

Informacijska varnost je upravljanje s tveganjem. Tega ne moremo popolnoma izključiti, zato smo stalno prisiljeni sklepati kompromise (Purser 2004c, 3).

2.3.1 Standardi s področja varovanja IS, virov in informacij

Standardi s področja informacijske varnosti zagotavljajo sistematični pristop njenega upravljanja. Vključujejo najboljše prakse nadzora, kvantificirajo raven še sprejemljivega tveganja in združujejo ustrezne mere, ki ščitijo zaupnost, integriteto in razpoložljivost informacij (Manik 2007, 2).

Najpomembnejši med obravnavanimi standardi so:

a) ISO/IEC 27001:2005
b) ISO/IEC 27002:2005
c) ISO/IEC 27005:2008

Standard iz točke a združuje sisteme za upravljanje varovanja informacij. Predstavlja nadgradnjo britanskega standarda BS 7799, osnovanega s strani BSI[4]. Zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje sistema za upravljanje varovanja informacij v organizaciji SUVI[5]. Sprejetje tega sistema mora biti strateška odločitev organizacije (ISO 2005a, iv). V točki b je standard z naborom možnih ukrepov za nadzor prepoznanih tveganj, ki so se z leti uporabe v različnih organizacijah po svetu pokazali kot primeri dobre prakse. V smislu informacijske varnosti sta omenjena standarda celovita. To pomeni, da ne obravnavata le informacijske tehnologije in informacij v

[3] SOX – angl: Sarbanes-Oxley Act 2002.
[4] BSI – angl: British Standard Institute.
[5] SUVI – Sistem za upravljanje varovanja informacij.

elektronski obliki, temveč so vključene tudi informacije v ostalih možnih oblikah in medijih. Vpeljava in certificiranje s standardom ISO 27001 temelji na rezultatih formalne ocene tveganja. Standard, naveden v točki c, predstavlja podporo standardu ISO/IEC 27001. Razdeljen je v več faz. Vsebuje številne dobre prakse, ki nas usmerjajo pri pripravi ocene tveganja. Posamezne faze osvetljujejo bistveni namen priprave ocene tveganja, njeno izvedbo, obravnavo in sprejetje tveganja, obveščanje ter spremljanje tveganja.

2.3.2 Ocene tveganja

Tveganje je kombinacija posledic, ki lahko sledijo pojavu neželenega dogodka in verjetnosti pojava tega dogodka. Za učinkovito obvladovanje vseh vrst tveganj, ki so prisotna na področju informacijske varnosti, je najprej treba napraviti oceno tveganja. Za pripravo ocene tveganja moramo upoštevati vse posebnosti organizacije. Ocena tveganja lahko služi v podporo organizaciji, ki se odloči za vzpostavitev učinkovitega sistema SUVI. Pripravo ocene tveganja lahko določajo zakonodaja, zahteve partnerjev ali strank. Vzrok je lahko vpeljava neprekinjenega poslovanja (upoštevanje priporočil PAS 56) ali odziv na možne incidente. Oceno tveganja lahko napravimo za nov proizvod ali storitev, ko zanj pripravljamo opis zahtev glede varovanja informacij.

Pri izdelavi ocene tveganja izberemo ustrezen, razumljiv in dovolj enostaven pristop. Izbrana metodologija mora biti razumljiva ne samo tistim, ki oceno tveganja pripravljajo, ampak tudi ostalim, ki jo bodo uporabili oz. bodo pri tem udeleženi. Zagotavljati mora, da bodo ocene dale primerljive rezultate, ki jih bo mogoče ponoviti oz. primerjati s predhodno opravljeno oceno tveganja. V skladu s strateško vrednostjo informacij, kritičnostjo IS, zakonskimi ali pogodbenimi zahtevami, pričakovanji lastnikov in ne nazadnje s posledicami na ugled organizacije izberemo merila za vrednotenje tveganja. Vpliv na izbiro imajo prav tako geografske značilnosti (potresno, poplavno območje itd.) pa tudi družbeno kulturno okolje organizacije.

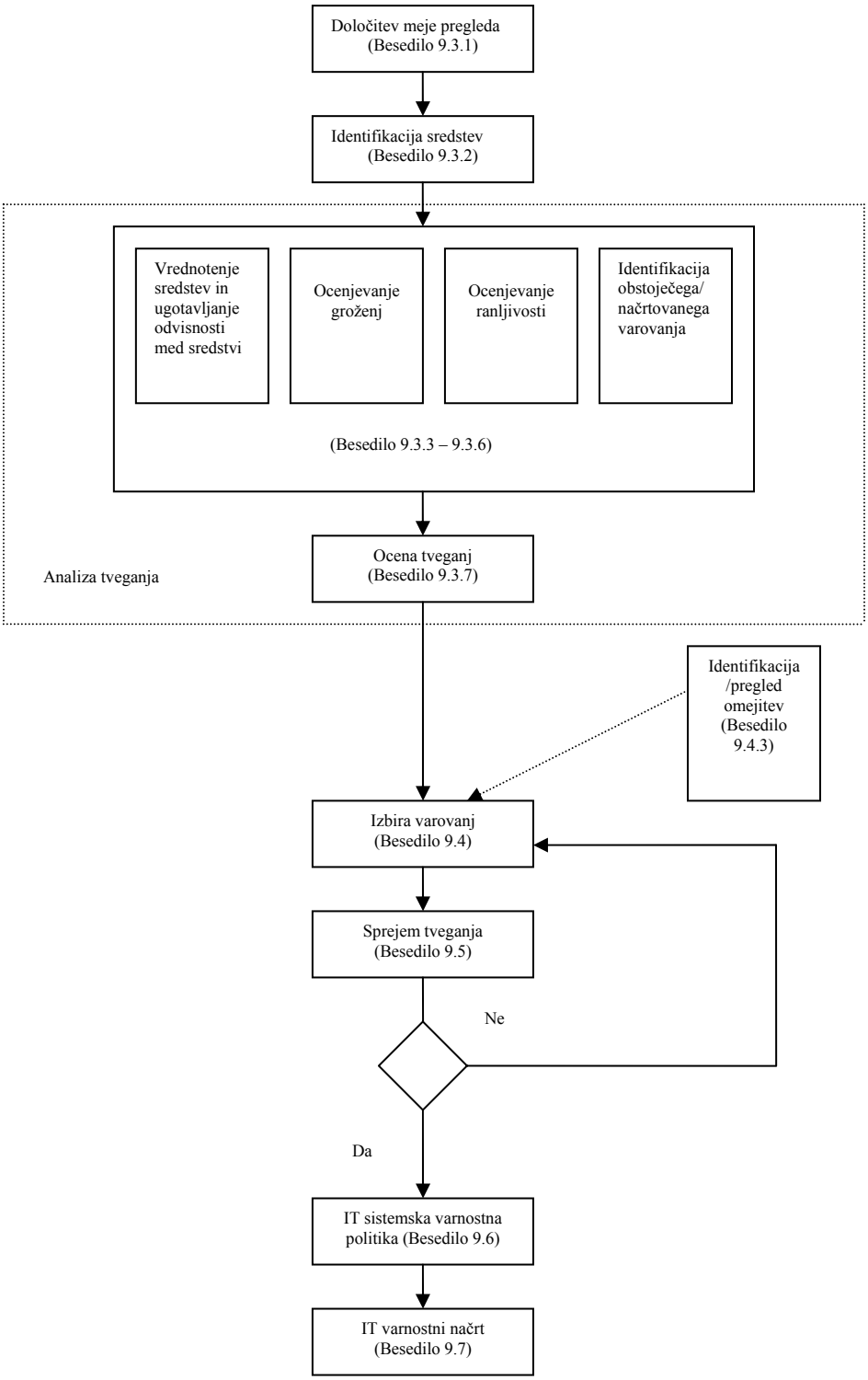
Ob začetnem preverjanju ocene tveganja so numerični podatki, s katerimi razpolagamo, večinoma neprimerni za kvantitativno izvedbo. V praksi se zato kot prvo uporabi kvalitativno ocenjevanje, priznano tudi s strani IT governance COBIT in standarda ISO (Likar et al. 2011; Trček 2006, 26). Za posamezne kategorije se uporablja opisne vrednosti kot nizko, srednje, visoko itd., prikazane v preglednici 1. S preglednico dobimo numerični rezultat kvalitativne ocene tveganja. Ocena velikosti tveganja je lahko npr. 1, 3, 6 ali pa tudi 0, če tveganja ni. Pri periodičnih ponovitvah ocen tveganja sčasoma poleg kvalitativne dodajamo še kvantitativno komponento, kjer uporabimo podatke preteklih primerov. Pomagamo si z ocenjevalnimi lestvicami in numeričnimi vrednostmi. Kvaliteta takšne analize je precej odvisna od kvalitete podatkov.

Preglednica 1: Matrika za ocenjevanje tveganj

Opis grožnje	Stopnja grožnje	N			S			V		
	Stopnja ranljivosti	N	S	V	N	S	V	N	S	V
Stopnja vrednosti vira	B	0	1	2	1	2	3	2	3	4
	M	1	2	3	2	3	4	3	4	5
	S	2	3	4	3	4	5	4	5	6
	V	3	4	5	4	5	6	5	6	7

B – brez; M – majhna; N – nizka; S – srednja; V – visoka.
Vir: Trček 2006, 26.

Ocena tveganja dejansko določi vrednost virov IS v skladu z njihovim pomenom za organizacijo. Na teh virih prepozna ranljivosti, ki obstajajo, in morebitne grožnje pa tudi kontrole, ki so že vzpostavljene, in njihov vpliv na obstoječe tveganje. Diagram poteka na sliki 3 prikazuje vzorčni primer natančne izdelave analize tveganja, objavljen v tehničnem poročilu mednarodne organizacije za standardizacijo (ISO 1998, 22).



Slika 3: Primer podrobne analize tveganja

Vir: ISO 1998.

Osrednji del analize vsebuje prepoznavo virov, ki so predmet tveganja. Sledi njihovo vrednotenje in ugotavljanje morebitne soodvisnosti med njimi. Nadaljuje z oceno ranljivosti in groženj na izbranih virih ter upošteva planirano obstoječe varovanje. Napravi oceno

tveganja. Določi prag še sprejemljivega tveganja in iz zbrane celote na koncu zasnuje IT varnostno politiko in IT varnostni načrt.

2.3.3 Varnostna politika in upoštevanje dobrih praks

Uporaba najrazličnejših sodobnih prenosnih in mobilnih komunikacijskih naprav ter vpetost v omrežje svetovnega spleta predstavlja odgovornim za informacijsko varnost v organizacijah dnevno nove izzive. Z varnostnega vidika so IS vse bolj izpostavljeni različnim nevarnostim in tveganjem. Upoštevati je treba vse možne oblike ranljivosti in groženj za IS znotraj organizacije kot tudi vse oblike ranljivosti pri njeni komunikaciji navzven.

Varnostna politika

Prvi korak, ki ga organizacija lahko napravi, da tovrstne nevarnosti zmanjša, je, da razvije in vzpostavi ustrezno varnostno politiko. Varnostna politika predstavlja krovni dokument varovanja informacij v organizaciji, zato morajo, če želijo uspešno varovati informacije, omenjeni dokument pripraviti in z njim seznaniti vse zaposlene (Židanik et al. 2004, 34). Zaposlene je treba tudi izobraževati o njihovih dolžnostih pri varovanju informacij.

Dokument mora predvideti jasna navodila za uporabnike IS, ki bodo določala pričakovano in sprejemljivo uporabo komunikacijskih naprav. Varnostna politika mora biti zasnovana tako, da omogoča stalne prilagoditve in izboljšave, skladno s spreminjajočim se poslovnim okoljem. V njeno pripravo morajo biti vključeni tudi zaposleni, ki niso člani IT skupine. To pripomore k temu, da bodo uvedeni varnostni postopki in politike bližje običajnim uporabnikom in s tem bolje sprejeti. Varnostna politika naj ne bi na račun varnosti po nepotrebnem ovirala dela uporabnikov na IS. Dobro je, da se po skrbnem pregledu vseh verjetnih tveganj dobi več možnih rešitev. Med temi se odgovorno osebje za pripravo politike odloči za tisto, ki najbolje zadosti pogojema varnosti in organizacijske učinkovitosti (Dhillon 2001, 9-13).

Sprejeto varnostno politiko je treba periodično preverjati, če se izvaja, kot je bila zamišljena. Ko so bile slovenske organizacije v raziskavi pred osmimi leti vprašane, kako preverjajo izvajanje svoje varnostne politike o varovanju informacij, jih je večina to izpeljala z nadziranjem dogajanja in beleženjem nenavadnih dogodkov. Sledilo je preverjanje omrežja in periodično revidiranje varnostnih procesov. Preverjanja pa sploh ni izvajalo petnajst odstotkov vprašanih organizacij (Židanik et al. 2004, 37).

Organizacija si mora pripraviti postopek preverjanja učinkovitosti vpeljane politike informacijske varnosti. To lahko stori že z analizo podatkov, ki jih zbira sama. Med take podatke štejemo interna revizijska poročila, zabeležene dogodke in pripombe, statistična poročila, log datoteke IS, rezultate analize tveganja, zapise internih izobraževanj, rezultate penetracijskih testov IS, odzive strank in interesnih skupin itd. Z dobljeno analizo je mogoče

v danem časovnem obdobju napraviti primerjavo s predhodnim stanjem in določiti smernice dodatnega izboljšanja za naprej (Hong-li in Zhu 2009).

Mednarodni standard ISO (2005b, 9) predlaga: "Politika varovanja informacij mora imeti lastnika, ki mu vodstvo potrdi odgovornost za razvoj, pregledovanje in vrednotenje varnostne politike. Pregled mora vključevati ocenjevanje možnosti za izboljšanje politike varovanja informacij v organizaciji in pristop k upravljanju varovanja informacij kot odgovor na spremembe v organizacijskem okolju, poslovnih okoliščinah, pravnih pogojih ali tehničnem okolju".

Dobre prakse

Celovito urejanje informacijske varnosti organizacij vsebuje varnostne politike s področja informacij in podatkovnega prenosa, ozaveščanje uporabnikov na seminarjih in tečajih, združeno s kontrolami delovnih postaj in mrežne infrastrukture. Mehanizmi učinkovite zaščite sistemov in podatkov so zapisani v več standardih s področja varovanja informacij kot tudi v objavljenih najboljših praksah iz industrije in ostalih področij. Učinkovito spopadanje s prepoznanimi tveganji v različnih organizacijah po svetu in pri nas ob sodelovanju vladnih, nevladnih organizacij, združenj in inštitutov je pripomoglo k oblikovanju številnih dokumentov s primeri dobrih praks. Omenjena je bila že publikacija COBIT, izdana s strani združenja revizorjev IS ISACA. Pri nas deluje slovenski odsek tega združenja, ki je skupaj s Slovenskim inštitutom za revizijo vzpostavil sistem opravljanja izpitov za nazive preizkušenih revizorjev IS. V svetu sta med ostalimi na tem področju zelo aktivna tudi SANS in NIST inštitut.

Za organizacije je priporočljivo, da so vključene v podobna strokovna združenja oz. da vzdržujejo kontakte z zainteresiranimi skupinami tega področja. Tako ostajajo v stiku z najbolj svežimi informacijami, si izmenjujejo znanje glede najboljših praks in izobražujejo svoje osebje, zadolženo za varnost IS. Najboljša praksa je seveda lahko koristna, da z njo preverimo rešitev, ki je bila zasnovana za izpolnitev določenih zahtev, vendar pa ne bi smela biti uporabljena za gonilo teh zahtev (Purser 2004c, 2).

3 METODOLOGIJA – PROAKTIVNI PRISTOP ZAGOTAVLJANJA VARNOSTI IS

Obravnavani pristop kombinirano dopolnjuje standarde informacijske varnosti in inovativno upravljanje varnosti. Predstavljena je inovativna metodologija upravljanja varnosti IS in informacij, ki pa ni nadomestilo za standardne metode varnosti.

3.1 Izbira ustrezne tehnike ustvarjanja idej med zaposlenimi za področje informacijske varnosti organizacij

Na temelju poznavanja principov ustvarjalnega mišljenja so psihologi razvili več tehnik. Skupne so si v tem, da skušajo pripraviti razmere, ki spodbujajo nastajanje idej. S tehnikami zmanjšujemo notranje in zunanje miselne bloke, vzpodbujamo igranje posameznih vlog, iskanje analogij itd. Gre za izrazito divergentno razmišljanje, kjer ni v igri ena sama rešitev problema, ampak se jih poskuša odkriti čim več. Za primerjavo lahko vzamemo konkavno lečo. Snop žarkov se ob prehodu skoznjo razprši. Podobno je tudi z razmišljanjem. En problem povzroči več različnih misli, asociacij in možnih rešitev (Likar 2002, 19). Pomembna je tudi ločenost procesov proizvajanja in preverjanja idej. Istočasno vrednotenje in ocenjevanje namreč zavreta ustvarjalne misli.

Ločimo posamične (individualne) in skupinske tehnike. Temeljijo na številnih skupnih kot tudi različnih principih. Temeljna razlika med skupinsko in posamično tehniko je v številu udeležencev. Z omenjenimi tehnikami tudi razvijamo, izpopolnjujemo, izbiramo in preverjamo ideje (Pečjak 1989, 17-19).

V teoretičnem modelu, na katerem temelji magistrsko delo, je bila predlagana uporaba skupinskih tehnik, pri katerih ustvarjalno skupino sestavljajo udeleženci iz različnih organizacijskih enot. Zato se lahko obravnava varnostna vprašanja v zvezi s posebnostmi različnih delov organizacije (Likar in Trček 2012).

3.1.1 Posamične tehnike

Pri individualnih tehnikah na osnovi znanega problema je posameznik nehote omejen z določenim svojim načinom razmišljanja in včasih težko izstopi iz tega kalupa. Po drugi strani pa nanj ne vplivajo miselne blokade, ki jih lahko izzovejo prisotnost ali neumestne izjave drugih udeležencev, kar je lahko primer v skupini. Med posamičnimi sta znani tehniki naključno izbranih besed in prisilne povezave (korelacije). Pri prvi naključno izbiramo besede in iščemo povezave med njimi. Naključje je torej treba ustvariti. Namen tehnike je, da se izognemo ustaljenim načinom razmišljanja in praksi iskanja rešitev v okviru znanega. S tehniko prisilne povezave pa se izognemo problemom, da rešitve pogosto postajajo zapletenejše, čim bolj poglobljeno znanje imamo o stvari, za katero jih iščemo (Likar, Križaj in Fatur 2006, 51). Temeljijo na dejstvu, da so številna odkritja pravzaprav naključje.

3.1.2 Skupinske tehnike

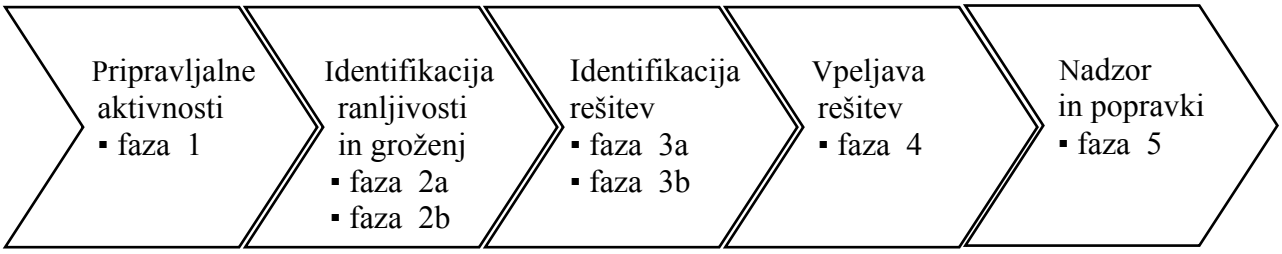
Skupinske tehnike, kot so burjenje možganov, možgansko pisanje (brain writting), Gordonova tehnika in podobno, vključujejo od 5-15 udeležencev. Za iskanje in ugotavljanje morebitnih varnostnih pomanjkljivosti v IS organizacije uporabljamo skupinske tehnike, izvajane na temelju znanega problema, in skupinske tehnike, kjer problema ne poznamo. Primer zadnje je Gordonova tehnika, kjer koncept problema zasnuje vodja. Prednost tega pristopa je originalnost idej. Zahteva dobro uigranost vodje. Pri delu v skupini udeleženci spodbujajo drug drugega h generiranju idej, pri čemer se sprosti zelo veliko ustvarjalnega potenciala. Prav tako laže dosežemo različnosti v mišljenju, ker vsakdo razmišlja nekoliko po svoje.

V našem primeru je problem znan. Iščemo varnostne pomanjkljivosti IS v dveh naključno izbranih ustanovah oz. organizacijah. Udeleženci se zato lahko takoj osredotočijo na znani vidik tega problema, tj. področje informacijske varnosti organizacije. Poznavanje problema običajno nekoliko vpliva na izvirnost dobljenih rešitev. Člani skupine se nehote zavedajo znanih težav, ki so povezane z določenimi možnimi predlogi, pa jih zato ne predlagajo. V prid tehniki na osnovi znanega problema govori tudi dejstvo, da večina udeležencev ni poznavalcev s področja informacijske varnosti. Zato niso omejeni z znanjem znanih problemov in rešitvami zanje.

Zaključimo lahko z ugotovitvijo, da so skupinske tehnike, ki temeljijo na znanem problemu, najbolj ustrezne. Odločili smo se za metodo viharjenja možganov oz. možgansko nevihto (brain storming) ameriškega psihologa Alexa F. Osborna, ki jo je prvič preizkusil že leta 1930 kot vodja reklamne agencije v New Yorku (Pečjak 1989, 23).

3.2 Prikaz vseh faz koncepta proaktivnega pristopa

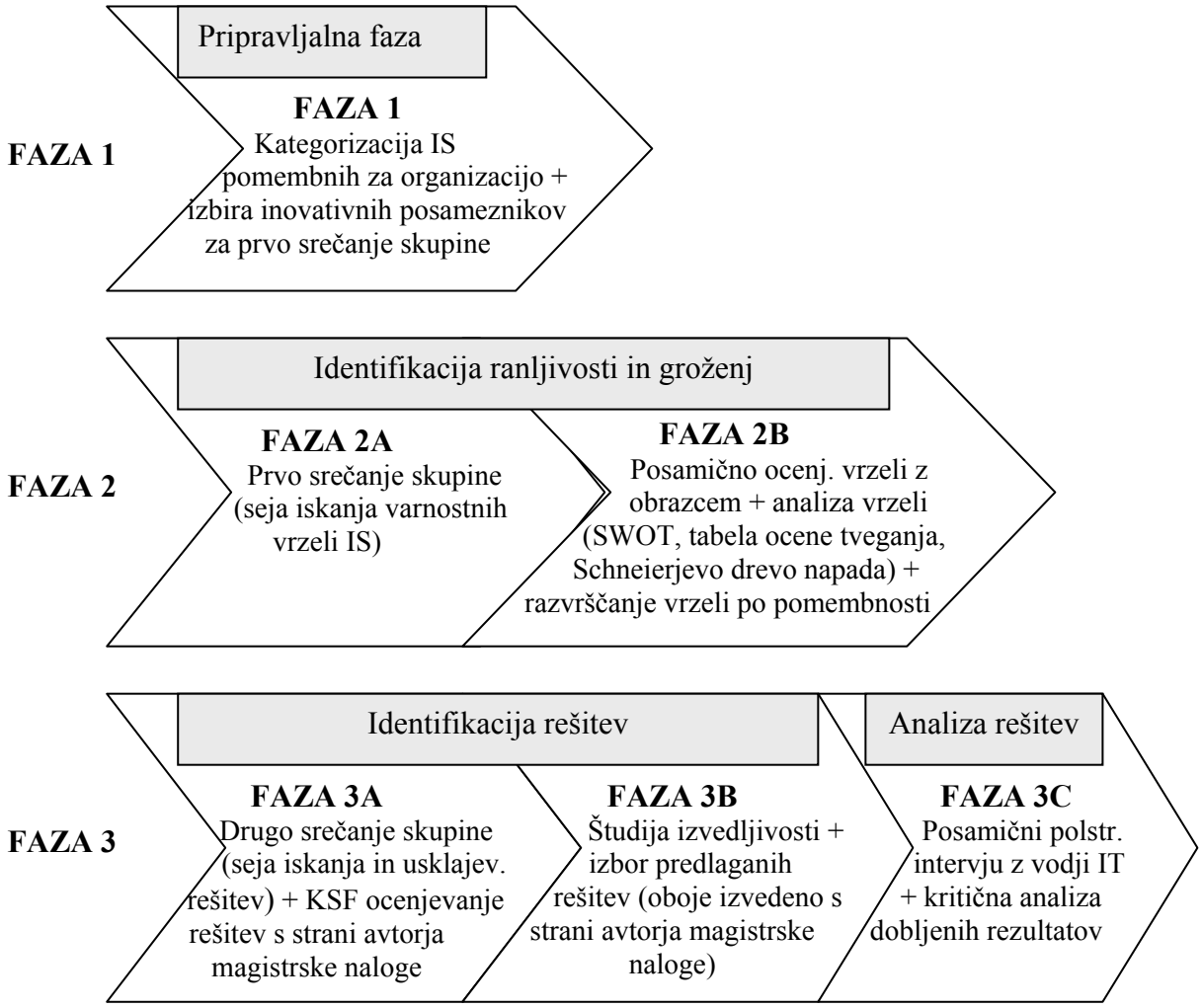
V skladu s predstavljenimi dejstvi iz prejšnje točke so faze izvajanja izvirne varnostne metodologije IS prikazane na sliki 4.



Slika 4: Faze proaktivnega procesa

Vir: Likar in Trček 2012.

Na uvodnem razgovoru v prvi organizaciji, kjer smo izvedli raziskavo, je vodja službe za informatiko izpostavil omejene časovne in kadrovske možnosti dela s skupino. Za organizacijsko in časovno sprejemljivo je označil dvakratno srečanje skupine. Prvo za sejo možganske nevihte (iskanje varnostnih vrzeli IS) in drugo za iskanje rešitev ocenjenih vrzeli IS. Temu dejstvu smo izvirno metodologijo na sliki 4 v drugi in tretji fazi nekoliko prilagodili, kot kaže slika 5. Na enak način smo raziskavo izpeljali tudi v drugi organizaciji.



Slika 5: Prilagojene faze izvirne varnostne metodologije IS

Izvirna metodologija predvideva v fazi 2B srečanje skupine poznavalcev svojega ožjega področja (programerje računalniških rešitev, sodelavce ali vodje finančnega oddelka, IT podpore, razvijalce itd.), ki ocenjujejo predloge varnostnih vrzeli IS prve skupine iz faze 2A. Glede na prej predstavljena dejstva smo se v organizacijah dogovorili, da bodo z njihove strani izbrani ocenjevalci (prav tako poznavalci oz. vodje svojih področij) predloge varnostnih vrzeli ocenili posamično v organizaciji, ocenjevalni obrazci pa bodo posredovani po elektronski pošti.

Prilagojena faza 3A se od osnovne metodologije razlikuje v tem, da se skupina za končni predlog rešitve posamezne varnostne vrzeli uskladi na samem srečanju. Pri iskanju in usklajevanju rešitev je treba upoštevati veljavne interne pravilnike, morebitne izdelane lastne rešitve, standarde, priporočila dobrih praks itd. Po osnovni metodologiji se v tem delu faze vsako od možnih rešitev vrzeli ocenjuje bodisi na kvantitativni ali kvalitativni podlagi. V našem primeru je predlagane rešitve varnostnih vrzeli s tremi v naprej izbranimi kriteriji ocenil avtor magistrske naloge po kvalitativni metodi KSF.

Po izvirni metodi se fazo 3B izpelje metodološko podobno kot fazo 2B. Poznavalci svojih ožjih področij se zberejo na srečanju, podrobneje proučijo izvedljivost predlaganih rešitev varnostnih vrzeli in z eno od izbranih metod izberejo rešitve za največje ugotovljene vrzeli IS.

V našem primeru, kjer smo delo s skupino prilagodili na dve srečanji, je podrobnejšo analizo izvedljivosti predlaganih rešitev z drugega srečanja skupine in analizo kvalitativnega ocenjevanja iz faze 3A izvedel avtor magistrske naloge. O dobljenih rešitvah za varnostne vrzeli IS in naših analizah je tekla beseda tudi z vodilnimi s področja IT v organizaciji na zadnjem obisku. Namenjen je bil posamičnemu polstrukturiranemu intervjuju in kritični analizi dobljenih rezultatov (Faza 3C). Pomembne dodatne informacije o predlaganih rešitvah smo dobili tudi na tem srečanju.

3.2.1 Faza 1 – pripravljalna

Pripravljalno fazo sestavljata dva bistvena cilja:

- kategorizacija informacijskih virov, prikazanih na sliki 1 oz. prilogi 2, ki so pomembna za organizacijo;

- izbira skupine inovativnih posameznikov med zaposlenimi, ki bodo sodelovali v kreativni seji iskanja varnostnih vrzeli IS v naslednji fazi.

Pomembni del faze predstavlja postopek izbire udeležencev izbrane tehnike ustvarjanja idej. Med kandidate naj bi uvrstili tiste, ki so neposredno povezani z obravnavano problematiko, pa tudi ostale, ki je ne poznajo. Ključnega pomena je, da v skupino vključimo ustvarjalne posameznike z različnih strokovnih področij in organizacijskih enot (Dhillon 2001, 11).

Če nam okoliščine le dopuščajo, razdelimo kandidate v dve podskupini. V eni so ljudje z globljim poznavanjem IT, v drugi pa tisti s stopnjo poznavanja IT navadnih uporabnikov. Delitveni postopek ustvarjalnosti lahko izvedemo iz situacije, tako da udeležencem na enem od pripravljalnih srečanj pokažemo na primer sponko za spenjanje papirja in jih vprašamo: "V kakšen namen bi to sponko še lahko uporabili?" (Pečjak 1989, 27; Likar in Trček 2012). Povprečno število idej je nekje med šest do osem. Posamezniki z velikim številom odgovorov (deset in več) so prav gotovo tisti, ki bodo tudi s področja naše problematike prispevali največ uporabnih predlogov. Takšne vključimo v sejo ustvarjalnega mišljenja. Pri končnem

oblikovanju skupine upoštevamo tudi, da je zastopanost kandidatov iz večine oddelkov organizacije in ravni v njih. Vključimo po možnosti oba spola različnih starosti.

Če izvedbo predlaganega koncepta načrtujemo kot zunanji izvajalec, kot v našem primeru, s kontaktnimi osebami oz. z izbranimi vodji ustanove kategoriziramo (razvrstimo) informacijske vire organizacije v skladu z njihovim največjim pomenom zanjo. Pri tem si pomagamo s preglednico v prilogi 2. Prosimo jih tudi za kratko predstavitev obstoječega stanja in trenutnega obvladovanja področja varnosti IS. Če je treba, podpišemo zavezujoč dokument o varovanju prejetih informacij in podatkov. Zaprosimo tudi za pisne dokumente, ki morda obstajajo (sprejete varnostne politike, prevzete dobre prakse, pravilnike s področja varovanja osebnih in drugih strateških podatkov organizacije itd.). Vse tako pridobljeno znanje in informacije so moderatorju seje viharjenja možganov v pomoč pri usmerjanju ustvarjalnega procesa iskanja šibkih točk, ranljivosti in groženj obstoječega IS organizacije. Glede na pomembnost prej razvrščenih virov sestavimo orientacijska vprašanja v smislu, kot je prikazano v prilogi 12. Vprašanja so v pomoč koordinatorju za usmerjanje poteka seje možganske nevihte v drugi fazi.

3.2.2 Faza 2 – iskanje in ocenjevanje varnostnih vrzeli IS

Fazo sestavljata dva dela:

- Faza 2A – iskanje varnostnih vrzeli obstoječega IS v organizaciji (1. srečanje skupine)

- Faza 2B – ocenjevanje dobljenih predlogov varnostnih vrzeli iz dela 2A (praviloma se izvede z zamikom nekaj dni, še posebej, če so med ocenjevalci tudi tisti, ki so sodelovali na 1. srečanju skupine). Ta del faze smo iz pojasnjenih razlogov prilagodili, kot sledi:

    a) posamično ocenjevanje v organizaciji z ocenjevalnimi obrazci (priloga 3) po kriteriju njihove pomembnosti oz. aktualnosti za informacijsko varnost;

    b) analiza ocenjenih vrzeli (izvedena s strani avtorja magistrske naloge) z vidika trenutnega obvladovanja tveganj (tabela ocene tveganja), morebitnih nevarnosti, slabosti (SWOT analiza) in približna vrednostna ocena škode (Schneierjevo drevo napada), ki jo ugotovljena varnostna vrzel lahko povzroči.

Cilj analize vrzeli (točka b) je dokončna razvrstitev vrzeli za nadaljnjo obravnavo, še posebej, če je teh veliko oz. so prejele enako oceno. Na drugem srečanju skupine, v fazi 3A, večino časa želimo nameniti iskanju rešitev le za najpomembnejše nevarnosti IS.

Faza 2A – iskanje varnostnih vrzeli obstoječega IS

Določi se koordinatorja seje, ki pozna osnove tehnike ustvarjalnega vodenja. Dobro mora biti seznanjen z obstoječo IT varnostjo v organizaciji. Varnostni specialist ali vodja službe za informatiko organizacije pred začetkom seje viharjenja možganov uvodoma poda kratko predstavitev obstoječe ravni informacijske varnosti v organizaciji. Gre za predstavitev na dovolj splošni ravni, da je lahko razumljena tudi tistim, ki niso specialisti s tega področja. Na seji možganske nevihte se s skupino vsaj petih udeležencev sistematično obdela prisotne in preteče ranljivosti IS ter možne varnostne grožnje. Avtorji metode število udeležencev navzgor omejujejo na petnajst (Pečjak 1989, 24). Za spodbujanje skupine so lahko v proces razmišljanja vključene tudi kulturne posebnosti organizacije. Preko igre tehnike vlog ustvarjalni proces lahko postane še bolj privlačen in učinkovit. Udeleženci se postavijo v vlogo vsiljivca in poskušajo najti izvirne načine za vstop v IS (Likar in Trček 2012, 6). Cilj tega dela faze je odkriti čim večje število sedanjih in bodočih (pretečih) varnostnih vrzeli obstoječega IS.

Faza 2B – ocenjevanje predlogov varnostnih vrzeli

Na začetku smo omenili, da vrednotenje in ocenjevanje predlaganih rešitev lahko zavreta ustvarjalne misli, zato ta del faze izpeljemo ločeno po preteku nekaj dni. Dobiti želimo kompetentne ocene. Pri tem naj bi poleg dela udeležencev iz prve skupine sodelovali poznavalci svojega ožjega področja (programerji računalniških rešitev, sodelavci ali vodje iz finančnega oddelka, IT podpore, razvijalci, raziskovalci, vodje varnostnikov itd.). Ocenjevalno skupino naj bi prav tako sestavljalo vsaj pet udeležencev.

V organizacijah, kjer smo izpeljali raziskavo, smo se na uvodnem srečanju z vodji zaradi omejenih časovnih in kadrovskih možnosti dela s skupino dogovorili, da bodo z njihove strani izbrani ocenjevalci predloge varnostnih vrzeli ocenili posamično v organizaciji, ocenjevalni obrazci pa bodo posredovani po elektronski pošti.

Naloga vsakega ocenjevalca je, da na poslanem ocenjevalnem obrazcu, ki je v prilogi 3, najprej intuitivno in po svoji presoji izbere pet do sedem boljših predlogov varnostnih vrzeli skupine z nevihte. Tri od teh nato da v ožji izbor in jih oceni s kriterijem pomembnosti oz. aktualnosti za informacijsko varnost v organizaciji, kot prikazuje preglednica 2.

Preglednica 2: Ocenjevanje vrzeli glede na njihovo pomembnost za inform. varnost

Številka predloga varnostne vrzeli	K (1-5)*

K – kriterij pomembnosti (aktualnosti) vrzeli na informacijsko varnost.
* Pomembnost oz. aktualnost vrzeli se ocenjuje z vrednostno oceno od 1 do 5 (5 je najbolj pomembna).

Iz ocen posameznih ocenjevalcev izračunamo in sestavimo matriko vseh ocenjenih predlogov. Številčno vrednost posameznega predloga vrzeli dobimo s seštevkom vrednosti kriterijev pomembnosti vseh ocenjevalcev, ki so ta predlog vrzeli izbrali v ožji krog in ga ocenili. V primeru, da dobimo veliko število predlogov za vrzeli IS, na seji možganske nevihte temu posledično sledi tudi večje število vseh ocenjenih predlogov. Nekateri med ocenjevanjem izpadejo (ne prejmejo nobene točke), ker se ocenjevalcem ne zdijo dovolj pomembni. Zgodi se tudi, da več ocenjenih predlogov prejme enako oceno.

Smiselno je, da izvajalec proaktivne metode v organizaciji ocenjene vrzeli analizira še z vidika trenutnega obvladovanja tveganj, morebitnih nevarnosti in slabosti ter napravi približno vrednostno oceno škode, ki jo ugotovljena varnostna vrzel lahko povzroči. Cilj tega je dokončna razvrstitev vrzeli za obravnavo na 2. srečanju skupine. Na podlagi dobljenih ocen se lahko vrzel, ki jo sicer ocenjevalci ocenijo slabše, glede pomembnosti njenega reševanja uvrsti više. Na drugem srečanju skupine, v fazi 3A, se pri iskanju rešitev za vrzeli želimo osredotočiti res na največje ugotovljene nevarnosti IS.

Z analizo SWOT v ocenjevalnih poljih presojamo prednosti, slabosti, priložnosti in nevarnosti za posamezno vrzel. Prednosti in slabosti zadevajo notranje, priložnosti in nevarnosti pa zunanje dejavnike organizacije. Vrzeli so same po sebi pomanjkljivosti. Presoja njihovih prednosti je mišljena v negativnem smislu. Ko v polja SWOT ocenjevalnega obrazca, ki je v prilogi 4, vpisujemo dejstva oz. odgovore na vprašanja, ki si jih pri posameznem predlogu vrzeli zastavljamo, si pomagamo s kriteriji, ki ustrezajo obravnavanemu viru (Likar et al. 2007, 46).

S pomočjo preglednice 1, na strani 15, ocenimo vrzeli še glede obvladovanja tveganj. Merilo pri uvrščanju tako obravnavanih predlogov vrzeli je večja stopnja tveganja (višja številčna vrednost iz tabele) za informacijsko varnost.

Varnostne vrzeli (v našem primeru smo izbrali prve tri), ki jim je pri ocenjevanju in analizi namenjena največja pozornost in prejmejo največ točk, tudi približno cenovno ovrednotimo. Za to oceno uporabimo Schneierjevo metodo drevesa napada (Schneier 2000, 318-333). Po analitičnem povzetku vseh treh ocen za posamezno vrzel se laže odločimo, kateri bomo dali prednost pri razvrščanju glede na pomembnost obravnave na 2. srečanju skupine. Še posebej to velja za vrzeli, ki po ocenah ocenjevalcev prejmejo enako število točk.

3.2.3 Faza 3 – iskanje in izbira rešitev vrzeli IS ter posamični polstrukturirani intervju z vodji IT in kritična analiza rezultatov

Prilagojena faza je deljena v tri dele:

- Faza 3A – iskanje in usklajevanje najboljših možnih rešitev za vsako izmed petih v predhodni fazi 2B ocenjenih in po pomembnosti razvrščenih varnostnih vrzeli IS (2. srečanje skupine)

  a) predlagane rešitve udeležencev skupine morajo upoštevati interne pravilnike, izdelane lastne rešitve, standarde in priporočila dobrih praks;

  b) vsaka od predlaganih rešitev je kasneje ocenjena po KSF metodi s strani avtorja magistrske naloge.

- Faza 3B – podrobnejša študija izvedljivosti predlaganih rešitev in dobljenih kvalitativnih ocen za posamezni predlog varnostne vrzeli s strani avtorja magistrske naloge

- Faza 3C – polstrukturirani intervju z vodji IT v organizaciji in kritična analiza doprinosa vseh treh za realizacijo predlaganih rešitev k informacijski varnosti

Faza 3A – iskanje rešitev varnostnih vrzeli IS

Skupino usmerja izbrani moderator (v našem primeru avtor magistrske naloge). S koordinatorji v organizaciji se dogovori, da jo večinoma sestavljajo udeleženci, ki so ocenjevali varnostne vrzeli. Pozornost je namenjena ugotovljenim največjim nevarnostim IS iz prejšnje faze. Izhajajoč iz dobljenih in ocenjenih ranljivosti virov udeleženci iščejo konkretne in hkrati najbolj učinkovite možne rešitve zanje. Predlagane rešitve morajo biti v skladu z internimi pravilniki, izdelanimi lastnimi rešitvami, standardi in priporočili dobrih praks oz. kombinacijami med vsemi. S skupino se na začetku dogovori, da se med več predlaganimi rešitvami za posamezno varnostno vrzel za njeno končno rešitev uskladi na samem srečanju. Na koncu faze dobimo za največje ugotovljene nevarnosti IS pet končnih predlogov rešitev skupine. Drugo srečanje je s tem zaključeno.

Sledi ocenjevanje vseh dobljenih rešitev za pet največjih vrzeli IS. Izvirna metodologija predvideva skupinsko ocenjevanje vsake od možnih rešitev bodisi na kvantitativni ali kvalitativni podlagi. V našem primeru smo izbrali kvalitativno metodo glavnih dejavnikov uspeha (KSF). V začetku poglavja smo omenili omejene časovne in kadrovske možnosti dela s skupino. Pri ocenjevanju rešitev igra vlogo predvsem časovna komponenta. Zato je ocenjevanje vseh predlaganih rešitev za obravnavane varnostne vrzeli prilagojeno in izpeljano s strani avtorja magistrske naloge.

Faza 3B – študija izvedljivosti in izbor rešitev varnostnih vrzeli IS

Cilj tega dela faze je izbira rešitev za varnostne vrzeli. Vključuje poglobljeno študijo izvedljivosti končnih predlaganih rešitev. V prilagojeni obliki je izvedena s strani avtorja magistrske naloge. Skladno s kvalitativno oceno, ugotovitvami in primerjavo s končnimi predlogi rešitev skupine se rešitve razvrsti v skladu s hitrostjo možne izvedbe in pomenom za informacijsko varnost. Za lažje odločanje pri razvrstitvi si lahko pomagamo tudi z ocenami iz tabele tveganja in vrednostnimi ocenami Schneierjeve metode drevesa napada iz dela faze 2B. Pri končni izbiri treh rešitev damo prednost tistim, ki so po KSF ocenjevanju najbolje uvrščene in hkrati sovpadajo s končnimi izbranimi rešitvami skupine.

Faza 3C – posamični polstrukturirani intervju z vodji IT in kritična analiza rezultatov

V zadnji del prilagojene tretje faze sta vključena posamični polstrukturirani intervju z vodji IT, vsake od obravnavanih organizacij in kritična analiza doprinosa vseh za realizacijo predlaganih rešitev k informacijski varnosti. Vprašanja polstrukturiranega intervjuja so predstavljena v prilogi 7.

3.2.4 Faza 4 – vpeljava predlaganih rešitev

Organizacija v tej fazi pristopi k vpeljavi z novo metodologijo poiskanih in izbranih predlogov rešitev. Vsaki predlagamo po tri. Gre za rešitve ranljivosti sistema IS, ki so šle skozi vse postavljene kriterije selekcije predhodnih treh faz. Ocenjene rešitve morajo organizacije pred uvedbo le še uskladiti s svojimi operativnimi in strateškimi pozicijami, skladno z upravljanjem s tveganji.

3.2.5 Faza 5 – spremljanje vpeljanih rešitev

Vpeljane predlagane rešitve je treba stalno spremljati in se hitro odzivati na morebitne nepredvidene spremenjene okoliščine ter sprejeti ustrezne popravne ukrepe. Prav temu je namenjena ta faza predstavljenega postopka.

Zunanje dinamično okolje organizacij in hitri tehnološki razvoj prinašata s seboj vedno nove izzive. Posledično to pomeni tudi drugačne varnostne grožnje in vse bolj prefinjene oblike ranljivosti IS. Celotni postopek na sliki 4 oz. 5 je zato smiselno na obdobje polovice leta ponoviti.

3.3 Pogostost izvajanja predstavljenega koncepta

Ponovitev opisanih faz se predlaga na vsakih šest do dvanajst mesecev (Likar in Trček 2012, 7). V prid temu govorijo tudi izsledki skupine Gartner. Trdijo namreč, da načrtovanje na

področju IS ni smiselno za več kot 24 mesecev vnaprej. Poleg tega je predvidevanje trendov čez to časovno obdobje pokazalo, da je obrobne vrednosti (Frick in All 2000).

Kadar se bistveno spremenijo okoliščine v organizaciji, kar je lahko posledica prevzema s strani druge organizacije, oz. če pride do ukinitve določenih organizacijskih enot, je prav tako smiselno osvežiti faze postopka. Popolnoma nove okoliščine dobimo tudi pri selitvi določenega programa organizacije na drugo lokacijo. Komunikacijska pot tedaj poteka bodisi preko posebne najete linije ali interneta. Če želimo proaktivno vplivati na novonastalo situacijo, je treba ponovno skrbno pregledati morebitne ranljivosti IS v spremenjenih okoliščinah. Še posebej velja natančno pregledati vse nastavitve mrežnih usmerjevalnikov, da res v celoti upoštevajo spremenjeno situacijo. Na ponovitve metode vpliva tudi na novo instalirana programska oprema, njeni popravki (posodobitve), zamenjava sistemske (strežniki) ali uporabniške opreme (delovne postaje), spremembe različnih električnih in mrežnih instalacij v obnovljenih poslovnih prostorih, priprave na periodično (letno) presojo morebitnega že pridobljenega certifikata o informacijski varnosti itd. Če bi metodologijo in rešitve dejansko uporabili v organizacijah, bi varnostne rešitve spremljali v daljšem časovnem obdobju (pol leta ali dlje). To bi zahtevalo longitudinalno študijo, kar pa presega okvir te magistrske naloge. Zato se omejimo le na prve tri faze predlaganega koncepta.

4 PREIZKUS INOVATIVNEGA KONCEPTA VAROVANJA IS V PRAKSI

Teoretični model povečanja varnosti IS iz točke 3.2 smo v nekoliko prilagojeni obliki preizkusili v dveh naključno izbranih organizacijah. Gre za originalen pristop, ki se v podjetniški praksi ne izvaja, zato smo skrbno pripravili vse faze dela. Najprej smo metodologijo in cilje ter potencialne koristi jasno predstavili vsem kontaktnim osebam v organizacijah in pridobili soglasje vodstva. Zaradi omejenih časovnih in kadrovskih možnosti dela s skupino smo se s koordinacijskimi vodji dogovorili, da se delo s skupino izvede dvakrat, prvič za sejo možganske nevihte (iskanje varnostnih vrzeli IS) in drugič za iskanje in usklajevanje rešitev za ocenjene predloge varnostnih vrzeli. Ocenjevanje predlogov vrzeli je s pomočjo ocenjevalnega obrazca potekalo v organizaciji. Večina ocenjevalcev je bila prisotna tudi pri iskanju in izbiri rešitev zanje. Selekcijo ustreznih kadrov za sodelovanje v posameznih fazah dela glede na potrebe metodologije in kompetence sodelujočih so izvedli v organizacijah samih. Za vse faze dela smo pripravili delovna izhodišča in gradiva, ta so prikazana v prilogah 1, 2, 3, 4 in 7. Ustrezno smo o podrobnostih pred začetkom obeh srečanj informirali tudi sodelujoče (možganska nevihta, ocenjevanje predlogov, iskanje in usklajevanje rešitev).

4.1 Izbira organizacij in ustreznega pristopa k izvedbi raziskave

V skupinski tehniki nevihte možganov, ki je uporabljena v nalogi, sestavlja skupino za iskanje možnih varnostnih pomanjkljivosti obstoječega IS vsaj pet udeležencev iz različnih oddelkov izbrane organizacije. Temu dejstvu je bila podrejena tudi izbira organizacij, v katerih smo izpeljali raziskavo. Povabili smo pet malih, tri srednje in šest velikih organizacij ter dve ustanovi. Prva je bila visokošolska, druga pa državna institucija. Iz treh malih organizacij nismo dobili nobenega povratnega odgovora, z enim od srednjih ni bilo iz neznanega razloga mogoče vzpostaviti kasnejšega kontakta z vodjo informacijskega področja. Iz dveh velikih organizacij prav tako ni bilo odziva, čeprav je bil predstavnikoma uprave na enem od IT dogodkov osebno predstavljen osnovni koncept. Iz preostanka velikih organizacij smo sicer dobili odgovore, vendar žal negativne. Enako velja tudi za obe ustanovi. Za pristop do ključnih ljudi v organizacijah (predsednikov uprav, direktorjev, vodij služb za IT, namestnikov direktorjev itd.) smo izkoristili številne komunikacijske poti (elektronsko pošto, internet, telefon, različne neodvisne strokovne dogodke, poznanstva iz preteklosti, predloge mentorja, informativne razgovore). V primeru da je šlo za osebni kontakt, jim je bil predstavljen celotni potek raziskave, časovni okvir in to, kaj z rezultati raziskave pridobi organizacija. Zaprosilu za raziskavo po elektronski pošti smo dodali priponko z opisom predvidenega plana raziskave. Besedilo je v prilogi 1.

Izkazalo se je, da v obdobju od druge polovice maja do začetka oktobra 2011 ni bilo mogoče najti nobene zainteresirane organizacije oz. ustanove, ki bi si vzela čas za raziskavo. Vzroki za to so bili različni: od razloga, da je čas dopustov in veliko ključnih kadrov manjka, do jasne opredelitve, da za to ni zanimanja. V večji proizvodni organizaciji je šlo za preobremenjenost vodje IT s tekočimi obveznostmi in zato posledično za njegovo popolno neodzivnost na našo elektronsko pošto, kljub dejstvu, da je raziskavi dala zeleno luč sama predsednica uprave. Na

eni od visokošolskih ustanov so člani kolegija brez dodatnega pojasnila sprejeli sklep, da se raziskavi ne ugodi. Iz popolnoma nerazumljivih razlogov ni prišlo do že praktično dogovorjenega začetka raziskave z enim od oddelčnih direktorjev srednje velike organizacije. Prošnjo za sodelovanje v raziskavi so na več nivojih in poslovnih področjih družbe preučili tudi v večji organizaciji s področja telekomunikacij, zavedajoč se, da takšno sodelovanje lahko prinese družbi določene koristi kot tudi potencialna tveganja. Pri tehtanju pozitivnih in negativnih učinkov na varnost IS in s tem povezanega poslovanja so se na koncu odločili, da prošnji po sodelovanju žal ne morejo ugoditi. Glede na občutljivo področje, ki ga obravnavamo v nalogi, so bili s strani ene od državnih institucij kljub predvidenemu dejstvu, da se podpiše zavezujoč dokument (pogodba) o varovanju pridobljenih informacij in da ime ustanove ne bo nikjer izpostavljeno, izraženi določeni pomisleki za sodelovanje v tovrstni raziskavi. Bolj optimistično je bilo elektronsko sporočilo iz uspešne organizacije s področja internetne prodaje. Posredovani predlog za raziskavo se namreč ni ujemal le z njihovim, že sprejetim letnim načrtom. Del podobnih aktivnosti so že opravili, del pa prestavili v leto 2013. Če bi bila naša ponudba v tem letu še aktualna, bi se celo priporočili za raziskavo.

Zaradi vseh omenjenih predhodnih dejstev smo raziskavo namesto v treh predvidenih organizacijah izpeljali v dveh. Obe sta srednje veliki organizaciji. Prva je proizvodno, razvojno in izvozno usmerjena za izdelke visoke dodane vrednosti. Druga je uspešna pri razvoju svojih produktov s pripadajočo programsko opremo. V partnerstvu je z znanimi svetovnimi proizvajalci programske in aparaturne opreme. Izvaja prav tako storitve z visoko dodano vrednostjo. Na področju varovanja informacij je nosilec certifikata ISO 27001:2005 s področja varovanja informacij o poslovnih partnerjih in internih informacij.

V obeh izbranih organizacijah se je za časovno, organizacijsko in kadrovsko sprejemljivo s strani vodstva in sodelujočih izkazalo, da ocenjevanje predlaganih varnostnih vrzeli s kreativne seje možganske nevihte izvede vsak ocenjevalec sam. Zanje smo zato pripravili preglednici 5 in 6 s kratkimi povzetki prvega srečanja. Ocenjevalni obrazec, prikazan v prilogi 3, je bil po elektronski pošti poslan kontaktnim osebam v organizaciji. Komunikacija je potekala preko obeh vodij služb za informatiko. Za vso logistiko ocenjevanja v organizaciji sta poskrbela sama. Dogovorjeni smo bili, da se nam preslikane obrazce ocenjevanja pošlje po elektronski pošti.

Na drugem srečanju, v prvem delu tretje faze, smo skupini predstavili rezultate ocenjevanja in uvrstitev predlogov varnostnih vrzeli po pomenu. Drugo srečanje je bilo namenjeno soočenju argumentov ocenjevanja in iskanju rešitev za prvih pet odkritih in analiziranih največjih nevarnosti IS. V prvi organizaciji sta se za najmanj moteča izkazala sreda in četrtek, in sicer sta obe srečanji potekali ob 13. uri. V drugi organizaciji je bil najugodnejši petek po 13. uri, saj so udeleženci večino svojih zadolžitev tekočega tedna že opravili. V obeh organizacijah so bili sodelujoči v skupinah aktivni in zelo dobro motivirani.

4.2 Potek raziskave v obeh izbranih organizacijah

Prvo raziskavo smo izpeljali v srednje veliki, razvojno, proizvodno in izvozno usmerjeni organizaciji za izdelke visoke dodane vrednosti, drugo pa v srednje veliki organizaciji, uspešni pri razvoju svojih izdelkov s pripadajočo programsko opremo, ki je v partnerstvu z znanimi svetovnimi proizvajalci programske in strojne opreme. Izvaja tudi storitve z visoko dodano vrednostjo. Je nosilec certifikata ISO 27001:2005 s področja varovanja informacij o poslovnih partnerjih in internih informacij.

4.2.1 Faza 1 – pripravljalna

Razgovor v prvi organizaciji je bil dogovorjen z vodjo službe za informatiko. Prisoten je bil tudi vodja sistemske administracije. Predstavili smo jima celotni postopek novega pristopa k informacijski varnosti, vključno s porabo časa zanj. Dogovorili smo se za izpolnitev obrazca kategorizacije, ki je v prilogi 2, in za termin prvega srečanja s skupino. Izmed naštetih kategorij sta na obrazcu izbrala pet najpomembnejših za njihovo organizacijo, kot sledi v preglednici 3. Na uvodnem srečanju z direktorjem druge organizacije smo predstavili celoten koncept proaktivnega varovanja IS. Direktorjev pristop do informacijske varnosti je bil že doslej zelo napreden in pragmatičen. Zaradi narave dela imajo zaposleni dnevno opravka z veliko količino osebnih in zaupnih podatkov. Ljudje smo zmotljivi, zato ti podatki, tudi po pomoti, kaj hitro lahko zaidejo v nepooblaščene roke. V organizaciji so zato temeljito pregledali in prilagodili svoje delovne procese do te mere, da so uspešno opravili presojo za pridobitev certifikata ISO 27001:2005. Biti nosilec tega certifikata pomeni obvezo, saj se je treba vsako leto znova potrjevati. Naš koncept proaktivnega pristopa informacijski varnosti je bil sprejet kot dopolnilo obstoječemu stanju in kot priprava smernic za novo presojo. Drugi, operativnejši razgovor, smo imeli z osebo, ki je bila odgovorna pri izvedbi vseh potrebnih aktivnosti za pridobitev certifikata ISO 27001:2005 (oseba A) in vodjo sistemske administracije IT (oseba B). Obema je bila predstavljena kategorizacija virov iz priloge 2, predvidenih za raziskavo. Izbrala sta sedem najpomembnejših za njihovo organizacijo, kot sledi v desnem stolpcu spodnje preglednice.

Preglednica 3: Kategorizacija informacijskih virov

Prva organizacija	Druga organizacija
Dokumentacijski podatki	Dokumentacijski podatki
Uporabniška programska oprema	Uporabniška programska oprema
Prenosni računalniki	Stacionarni in prenosni računalniki
Elektronska sporočila	Komunikacijska programska oprema
Zaposleni	Strežniki
	Podatkovne baze
	Tržni delež

Rezultati izbire v obeh organizacijah kažejo razen pri dokumentacijskih podatkih, uporabniški programski opremi in prenosnih računalnikih na različna področja IS. V skladu z izbiro virov pri kategorizaciji moderator seje pripravi vprašanja o ranljivosti virov v naslednji fazi. Izbiro virov je zato potrebno napraviti skrbno, z dobrim poznavanjem razmer IT v organizaciji.

4.2.2 Faza 2 – iskanje in ocenjevanje varnostnih vrzeli IS

Faza je sestavljena iz dveh delov, 2A in 2B, kot je prikazano na sliki 5 na strani 21.

Faza 2A – iskanje varnostnih vrzeli obstoječega IS (1. srečanje skupine)

Srečanje skupine v prvi organizaciji je bilo v sredo ob 13. uri. Vodja službe za informatiko je za začetek napravil kratek uvod in povzetek našega prvega sestanka ter pojasnil, kakšen je namen srečanja. Potem je besedo prepustil nam in nas v sejni sobi pustil same. Pečjak (1989, 24) trdi: "Udeleženci se morajo počutiti povsem svobodne in samostojne. Nekateri avtorji ne priporočajo predstojnikov ali oseb, ki so v hierarhiji visoko nad udeleženci, npr. direktorjev, predstojnikov ali med študenti skupine profesorjev. Njihova prisotnost naj bi aktivirala človeškega cenzorja in zavrla svobodo mišljenja." V drugi organizaciji je oseba A (predstavljena v prejšnji točki) pred skupino desetih zaposlenih napravila kratek uvod. Predstavila je namen srečanja in cilje, ki jih želimo doseči. V uvodu je izpostavila tudi, da kupci vse pogosteje, preden se odločajo za naročilo storitev oz. nakup produktov, pošiljajo v organizacijo najrazličnejše vprašalnike. Z odgovori nanje želijo dobiti potrditev, ali so bile v organizaciji napravljene ustrezne analize interne informacijske varnosti. O nakupu oz. naročilu projekta se odločajo na osnovi potrditve, da se organizacija v resnici tudi ravna po rezultatih teh analiz. Poleg trga omenjeno smer vedno bolj narekuje tudi zakonodaja. Izbira skupine je bila v domeni ožjega vodstva organizacije. Med udeleženci so bili tudi zaposleni, ki so sodelovali na projektu pridobitve certifikata ISO 27001:2005. Že takrat so pri odločitvi izbirali med tistimi, od katerih so pričakovali največji prispevek. V spodnji preglednici so našteti oddelki iz katerih so bili udeleženci prvega srečanja.

Preglednica 4: Udeleženci skupine prvega srečanja prikazani po oddelkih

Prva organizacija	Druga organizacija
Razvoj	Razvoj
Prodaja	Marketing/prodaja
Finance	Sistemska administracija (2)
Kakovost	Produktno vodenje
Nabava	Razvoj strojne opreme
	OE rešitve
	Servis
	Kadrovski management
	Generalni direktor

Kreativna seja je trajala približno eno uro v prvi in dobrih petinštirideset minut v drugi organizaciji. S skupinama smo uspeli zbrati potencialne varnostne vrzeli IS, kot so prikazane v preglednicah 5 in 6.

Preglednica 5: Rezultati predlogov ranljivosti obstoječega IS (1. org.)

Možne ranljivosti	Povzetki komentarjev skupine in dodatne opombe
1 Neurejen arhiv (poplavno področje tovarne)	
2 Dokumentacija pri dobaviteljih	Dostopnost in pravila igre.
3 Zamenjava IS kupca	Eden izmed kupcev je pričel z menjavo IS. Moten je bil utečeni informacijski kanal z njim.
4 VPN[6] dostopi do omrežja organizacije	Obstajajo dostopi nekaterih zaposlenih "od zunaj" (preko oddaljenega dostopa) v omrežje organizacije. Stvar ni ustrezno dokumentirana in določena (upravičenje).
5 Izklapljanje delovnih postaj	Uporabniki po odhodu iz službe ne izklapljajo delovnih postaj oz. se z njih ne odjavijo.
6 Uganljiva standardna gesla	Za prijavo v omrežje se uporabljajo standardna gesla, ki se lahko uganejo (ni periodike menjav).
7 Nadomeščanje v času odsotnosti	V času službene odsotnosti uporabnikov se njihova prijava na sistem oz. uporabniški program uporablja s strani ostalih uporabnikov.
8 Dostop do ERP sistema (kalkulacije, planski podatki)	Uporabniki lahko izvajajo na ERP sistemu akcije, za katere morda niso pooblaščeni (upravičeni).
9 Instalacije programske opreme (administratorska pooblastila)	Uporabniki lahko sami instalirajo programsko opremo (kontrola upravičenosti nosilcev administratorskih gesel na delovnih postajah).
10 Uporaba prenosnikov izven delovnega mesta	Prenosniki se odnašajo z lokacije organizacije.
11 Uporaba prenosnikov za privatne zadeve (certifikati)	Službeni prenosni računalniki v uporabi za recimo spletno bančništvo z instaliranim certifikatom.
12 Kraja prenosnika	Glede na to, da se odnašajo izven organizacije, obstoji možnost odtujitve (iz avta ipd.).
13 Zunanje diskovne enote, USB ključi	Na njih so tudi službeni podatki. Možnost odtujitve.
14 Odslužena računalniška oprema (podatkovni nosilci)	Postopki odstranjevanja službenih podatkov pred odpisom oz. odvozom.

[6] VPN – angl: Virtual Private Network.

Možne ranljivosti	Povzetki komentarjev skupine in dodatne opombe
15 Osnovni viri (evidence, na terenu, reverzi)	Računalniška oprema večkrat menja lastnika. Stanje v evidencah ni istovetno s stanjem na terenu.
16 Izpisi (Rezalniki)	Ravnanje z neaktualnimi računalniškimi izpisi.
17 Papirna dokumentacija (Tiskalniki)	Računalniški izpisi, pozabljeni na tiskalniku, ipd.
18 Prodajna služba, nabavna služba in ostale v komuniciranju navzven	Omenjene službe naj bi sprejele kodeks, po katerem komunicirajo navzven vsaka le svoje področje (npr. cene ipd.).
19 Shranjevanje lastnih projektov na strežnik	Razvojniki naj bi svoje projekte iz stacionarnih postaj redno kopirali na ustrezno določeno strežniško lokacijo.
20 Ozaveščanje uporabnikov o prejemu "čudnih" elektronskih sporočil	Sumljiva elektronska sporočila s priponkami tudi od znanih naslovnikov (zloraba identitet).
21 FTP[7] dostop za kupce	Dostop do datotek preko FTP strežnika kupcem (prijava, zaščita).
22 Baza znanja; dokumentiranje zasnov (idej)	Znanje je v glavah in se premalo pretaka po organizaciji (pomanjkanje strukturnega kapitala, ki postane last organizacije).

Preglednica 6: Rezultati predlogov ranljivosti obstoječega IS (2. org.)

Možne ranljivosti	Povzetki komentarjev skupine in dodatne opombe
DOKUMENTACIJSKI PODATKI	
1 Pridobitev uporabniškega imena in gesla	Nekateri dokumenti v organizaciji so strogo zaupni. Pri dokumentih nam gre za zaščito sledljivosti kdo, kdaj in kako je popravljal te dokumente. Je bil za to pooblaščen? Certifikat ISO 27001:2005 zahteva trenutno tri-nivojsko zaščito z vlogami interno, zaupno, strogo zaupno. Govora je bilo o tem, kako bi nekdo, ki ni pooblaščen, prišel do strogo zaupnega dokumenta. Rečeno je bilo, da lahko od nekoga dobi uporabniško ime in pa geslo oz. da pride do profila uporabnika, kjer je natisnjen ta dokument ali celo do medija, kjer je shranjen.
2 Natisnjeni dokumenti na tiskalniku	Ta predlog se nanaša na predhodnega, torej, ko je bil zaupni dokument dan v tiskanje na tiskalniško vrsto. Med tem je na tiskalniku prišlo do zastoja papirja (paper jam). Vsi podatki so še vedno na disku tiskalnika oz. v njegovem internem spominu. Oseba, ki je odpravila zastoj papirja, morda ni med pooblaščenci natisnjenega dokumenta. Tiskalnik ga je pač natisnil takoj, ko je bil zastoj papirja odpravljen (v skladu s tiskalniško vrsto). Tiskalnik je na hodniku. Mimo njega hodi stalno veliko ljudi. Nekdo lahko stoji poleg tiskalnika in vzame natisnjen dokument pred tistim, ki ga je dal v tiskanje.

[7] FTP – angl: File transfer protocol.

Možne ranljivosti	Povzetki komentarjev skupine in dodatne opombe
3 Brisanje diskov tiskalnikov	Tudi ta predlog se nanaša na predhodna dva. Tiskalniki shranjujejo podatke za tiskanje na svojem internem disku. Ti diski se ne brišejo. Problem obstaja lahko tudi v primeru, ko gre tiskalnik na servis.
PODATKOVNE BAZE	
4 Varnostne kopije baze	Varnostne kopije podatkovne baze. (Recimo trak se nese na banko k stranki, kjer se ga lahko nepooblaščeno prekopira.)
5 Posodabljanje ORACLE baze	Varnostne "luknje" relacijske baze ORACLE in njihovo sprotno "krpanje".
UPORABNIŠKA PROGRAMSKA OPREMA	
6 Pravilna konfiguracija varnost. elementov omrežja	Pravilna konfiguracija CISCO opreme (usmerjevalnikov).
KOMUNIKACIJSKA OPREMA	
7 Spremljanje vrzeli na komunikacijski opremi	Sprotno spremljanje posodobitev opreme (angl: firmware) požarnih zidov, stikal, usmerjevalnikov itd.
8 Kontrola dostopa do konfiguracijske opreme	Kontrola, kdo in kdaj dostopa do te opreme. (recimo sled povezave do te opreme v internem omrežju s strani zaposlenega, s katere delovne postaje oz. prenosnika).
STREŽNIKI	
9 Sistemski prostor (sistem zavarovanja)	Možnost napačno instaliranega varnostnega sistema s strani zunanjega izvajalca, ki ga ni moč testirati. Lahko pa pri varnostnem preizkusu povzroči neljubi dogodek, kar se je že dogajalo drugje.
10 Strukturni kapital	Nadomestljivost zaposlenih v primeru odsotnosti. Koliko so postopki posameznikov, ki imajo specifične zadeve "v glavah", zapisani v neki bazi znanja, ki je dostopna preko gesel v takšnih izjemnih primerih. Dokumentiranje znanja zaposlenih. Znanje na ta način ostane v organizaciji, tudi če jo ti v prihodnosti zapustijo.
STACIONARNI IN PRENOSNI RAČUNALNIKI	
11 Kraja prenosnika, medijev USB itd.	Uporabniki, ki prenosnike in tovrstne medije potrebujejo za delo na terenu. Rečeno je bilo tudi, koliko časa se izgubi, da se ponovno vzpostavi uporabnikovo delovno okolje na novem prenosniku, če bi bil recimo stari odtujen (nove instalacije, nastavitve profila itd.)
12 Pametni telefoni	Kraja takšnega telefona. Na njem so (predvsem pri najbolj odgovornih v organizaciji) številni kontaktni podatki in tel. številke posl. partnerjev, oseb, elektronska pošta, ker je delo danes brez tega nepredstavljivo (24/7 razpoložljivost, hkratna udeležba recimo na seminarju, pomembnem sestanku in občasno spremljanje in usklajevanje dela projektne skupine nekje na terenu).
13 Pozabljene ponudbe	Po delu na terenu ostane ponudba recimo na disku prenosnika itd.

Možne ranljivosti	Povzetki komentarjev skupine in dodatne opombe
14 Socialna omrežja (odprtost)	Pametni telefoni s privzetimi nastavitvami. Samodejni priklop na kako zunanjo storitev ponudnika, če uporabnik tega ni vešč. Ne da uporabnik kaj stori, pride lahko že do kakega pretoka podatkov ali celo instalacije na mobilniku. Stalna sledljivost, (GSM cona), itd.
15 Zaposleni (previdnost glede polnega zaupanja 15 Zaposleni (previdnost glede polnega zaupanja novo zaposlenim)	Prihod novozaposlenega. Takojšnje zaupanje starozaposlenega in predaja gesla za dostop do nekega strežnika.
16 Zmotljivost (splošno ali kot posledica utrujenosti, preobremenjenosti itd.)	Dnevno se komunicira po elektronski pošti z veliko kontakti (tudi 100 in več). Pri tipkanju elektronskega naslova lahko ne vedoč pride do napake. Lahko gre za osebi z enakim imenom iz dveh različnih organizacij. Tako lahko neki dogovor, predlog pogodbe ali ponudba pride v napačne roke ali celo h konkurenci.

Predlogi ranljivosti druge organizacije v primerjavi s prvo zadevajo opazno višjo raven virov (pametni telefoni, usmerjevalniki komunikacijskega prometa, požarni zidovi, strukturni kapital itd.). Organizacija že dobro leto posluje v skladu s pridobljenim mednarodnim certifikatom ISO 27001:2005. Arhiviranje podatkov, ki se še kaže kot problem pri prvi organizaciji, je morala urediti tako, kot to zahteva omenjeni standard.

Faza 2B – ocenjevanje predlogov varnostnih vrzeli

Vrednotenje in ocenjevanje predlaganih ranljivosti lahko zavreta ustvarjalne misli, zato se to fazo izpelje po preteku nekaj dni. Ker želimo dobiti kar se da kompetentne ocene, na ocenjevanje poleg dela udeležencev iz prve skupine povabimo še poznavalce svojega ožjega področja (programerje računalniških rešitev, sodelavce ali vodje iz finančnega oddelka, IT podpore, razvijalce, raziskovalce, varnostnike itd.). Skupino naj bi prav tako sestavljalo vsaj pet udeležencev. V primeru da smo bili mi izvajalci proaktivne metode, se je za časovno sprejemljivo in zaradi omejenih kadrovskih možnosti dela s skupino s strani sodelujočih organizacij izkazalo, da ocenjevanje predlaganih varnostnih vrzeli izvede vsak ocenjevalec sam. Kriterij ocenjevanja je bil pomembnost dobljenih predlogov vrzeli na informacijsko varnost v organizaciji. Ocene posameznikov so lahko odvisne tudi od tega, iz katerega oddelka kdo prihaja, oz., katero funkcijo v organizaciji opravlja. S tega področja so si namreč pridobili največ izkušenj in kompetenc. Ta podatek je bil naveden na ocenjevalnem obrazcu. Koordinatorjem v organizacijah so bili po elektronski pošti poslani ocenjevalni obrazci (priloga 3) in preglednici 5 za prvo oz. 6 za drugo organizacijo. Sami so izbrali kandidate ocenjevalne skupine in jim obrazce posredovali. Tako je bilo ocenjevalcem omogočeno, da so ocenili predloge v času, ki jim je najbolje ustrezal. Tudi delovni proces je bil s tem najmanj moten. Izpolnjene obrazce smo preslikane dobili vrnjene nazaj. Do drugega srečanja s skupino, v tretji fazi, smo napravili izračun ocenjevanja in razvrstitev predlogov varnostnih vrzeli po pomembnosti za informacijsko varnost. To je bil tudi kriterij ocenjevanja predlogov. Ocenjevanje varnostnih vrzeli je bilo zaključeno v roku tedna dni. Rezultate ocenjevanja in

zastopanost ocenjevalne skupine po oddelkih prikazujejo preglednice 7, 8, in 9 za prvo oz. preglednice 10, 11 in 12 za drugo organizacijo.

Preglednica 7: Ocenjevanje vrzeli in zastopanost ocenjevalcev po oddelkih (1. org.)

Ocenjevalec	5-7 intuitivno izbranih predlogov							P1	KP1	P2	KP2	P3	KP3
Kakovost	1	7	17	4	5	–	–	1	5	4	5	5	4
Finance	11	9	1	8	17	–	–	11	5	8	4	1	4
Logistika	8	15	18	2	5	6,7*	9	6,7	5	8	5	15	5
Nabava	2	4	6	8	12	13	18	2	3	4	4	12	3
Razvoj	5	6	8	15	17	19	22	8	4	17	3	19	3
Prodaja	1	8	18	2	7	17	4	1	4	8	4	18	3
IT	4	9	20	13	12	–	–	4	4	9	4	20	3

* Ocenjevalec je vpisal in ocenil dva predloga.
P1, P2, P3 – trije izbrani predlogi vrzeli za ocenjevanje.
KP1, KP2, KP3 – kriterij pomembnosti (aktualnosti) predloga vrzeli (vrednostna ocena od 1 do 5; 5 je najbolj pomemben).

Preglednica 8: Skupni rezultati ocenjevanja varnostnih vrzeli (1. org.)

Št. predl.	Kakovost	Finance	Logistika	Nabava	Razvoj	Prodaja	IT	Vsota
8		4	5		4	4		17
1	5	4				4		13
4	5			4			4	13
6			5					5
7			5					5
11		5						5
15			5					5
5	4							4
9							4	4
17					3			3
19					3			3
2				3				3
18						3		3
20							3	3
12				3				3

Št. predl. – številka predloga, dobljena s kreativne seje možganske nevihte.

Preglednica 9: Ocenjeni predlogi varnostnih vrzeli po pomenu (1. org.)

Začetni vrstni red	Vrstni red po SWOT oceni	Št. predloga s 1. seje skupine	Ime predloga vrzeli	Št. točk
1	1	8	Dostop do ERP sistema (kalkulacije, planski podatki)	17
2	2	1	Neurejen arhiv (poplavno področje tovarne)	13
3	3	4	VPN dostopi do omrežja organizacije	13
4	6	6	Uganljiva standardna gesla	5
5	4	7	Nadomeščanje v času odsotnosti	5
6	7	11	Uporaba prenosnikov za privatne zadeve (certifikati)	5
7	5	15	Osnovni viri (evidence, na terenu, reverzi)	5
8	8	5	Izklapljanje delovnih postaj	4
9	9	9	Instalacije programske opreme (administratorska pooblastila)	4
10	10	2	Dokumentacija pri dobaviteljih	3
11	11	12	Kraja prenosnika	3
12	12	17	Papirna dokumentacija (tiskalniki)	3
13	13	18	Prodajna služba, nabavna služba in ostale v komuniciranju navzven	3
14	14	19	Shranjevanje lastnih projektov na strežnik	3
15	15	20	Ozaveščanje uporabnikov o prejemu "čudnih" elektronskih sporočil	3

Preglednica 10: Ocenjevanje vrzeli in zastopanost ocenjevalcev po oddelkih (2. org.)

Ocenjevalec	5-7 intuitivno izbranih predlogov							P1	KP1	P2	KP2	P3	KP3
Izv. reš.1	10	2	12	7	4	–	–	10	4	2	4	12	3
Izv. reš.2	10	2	12	7	4	–	–	10	4	2	4	12	3
Izv. reš.3	1	4	6	7	9	–	–	1	4	6	4	9	4
OE reš.	11	12	1	2	7	–	–	7	5	12	5	1	5
Trž. 1	3	4	7	8	11	12	6	6	5	11	4	4	5
Trž. 2*	10	11	12	16	2	–	–	10	4	12	4	–	–
Servis	10	12	6	15	16	–	–	6	3	15	3	16	2
OE sist.	6	7	10	11	12	15	16	11	4	7	4	15	3
Sist. adm.	12	5	6	8	9	–	–	12	4	5	5	9	4
Sistemi	11	12	2	3	4	–	–	11	4	12	3	3	5

P1, P2, P3 – trije izbrani predlogi za ocenjevanje.
KP1, KP2, KP3 – kriterij pomembnosti (aktualnosti) predloga vrzeli (vrednostna ocena od 1 do 5; 5 je najbolj pomemben).
Izv. reš. – izvedbene rešitve; sist. adm. – sistemska administracija.
OE reš. – OE rešitve; OE sist. – OE sistemi.
Trž. – trženje; * Ocenjevalec je ocenil le dva predloga.

Preglednica 11: Skupni rezultati ocenjevanja varnostnih vrzeli (2. org.)

Št. predl.	Izv. reš. 1	Izv. reš. 2	Izv. reš. 3	OE reš.	Trž.1	Trž.2*	Servis	OE sist.	Sist. adm.	Sistemi	Vsota
12	3	3		5		4			4	3	22
6			4		5		3				12
10	4	4				4					12
11					4			4		4	12
1			4	5							9
7				5				4			9
2	4	4									8
9			4						4		8
15							3	3			6
3										5	5
4					5						5
5									5		5
16							2				2

* Ocenjena sta bila le dva predloga.
Št. predl. – številka predloga, dobljena s kreativne seje možganske nevihte.
Izv. reš. – izvedbene rešitve.
OE reš. – OE rešitve.
Trž. – trženje.
OE sist. – OE sistemi.
Sist. adm. – sistemska administracija.

Preglednica 12: Ocenjeni predlogi varnostnih vrzeli po pomenu (2. org.)

Začetni vrstni red	Vrstni red po SWOT oceni	Št. predloga s 1. seje skupine	Ime predloga vrzeli	Št. točk
1	1	12	Pametni telefoni	22
2	2	6	Pravilna konfiguracija varnostnih elementov omrežja	12
3	3	10	Strukturni kapital	12
4	4	11	Kraja prenosnika, medijev USB itd.	12
5	6	7	Spremljanje vrzeli na komunikacijski opremi	9
6	5	1	Pridobitev uporabniškega imena in gesla	9
7	8	2	Natisnjeni dokumenti na tiskalniku	8
8	7	9	Sistemski prostor (sistem zavarovanja)	8
9	9	15	Zaposleni (previdnost glede polnega zaupanja novozaposlenim)	6
10	10	3	Brisanje diskov tiskalnikov	5
11	11	4	Varnostne kopije baze	5
12	12	5	Posodabljanje ORACLE baze	5
13	13	16	Zmotljivost (splošno, posledica utrujenosti, preobremenjenosti itd.)	2

Splošna analiza varnostnih vrzeli IS (1. org.)

Z analizo med vrzelmi izberemo res najpomembnejše za obravnavo na 2. srečanju skupine. V preglednici 7 se jasno vidi, katerim predlogom so posamezni ocenjevalci iz različnih oddelkov prve organizacije dali prednost in kako so ocenjevali pomembnost vrzeli na informacijsko varnost. Ocenjevanje kriterija pomembnosti je precej odvisno od poznavanja in kompetenc posameznikov za določeno področje. Glede na to da so bili na ocenjevanju prisotne vodje posameznih področij, je sklepati, da smo dobili realne in kvalitetne ocene tega kriterija.

Večje število predlogov vrzeli IS s seje možganske nevihte pomeni tudi verjetnost večjega števila vseh ocenjenih predlogov. Po ocenjevanju nekateri predlogi izpadejo, ker se ocenjevalcem ne zdijo dovolj pomembni. Zgodi se tudi, da več ocenjenih predlogov prejme enako oceno, kot na to opozarja primer v preglednicah 9 za prvo in 12 za drugo organizacijo. Predlogi z enakim številom točk v preglednicah še niso razvrščeni po prioriteti reševanja, temveč le po vrstnem redu njihovega nastanka na prvem srečanju skupine. Dokončno razvrstitev oz. prioriteto obravnave predlogov za 2. srečanje skupine dobimo z njihovo analizo, v našem primeru izvedeno s strani avtorja magistrske naloge. Izvajalec predstavljene metode se lahko odloči, kolikšnemu številu predlogov vrzeli bo namenil nadaljnjo pozornost. V nalogi smo se odločili za prvih osem ocenjenih predlogov. Najprej jih analiziramo s SWOT oceno. Predloge, ki imajo enako število točk, z dodatnimi argumenti laže pravilno razvrstimo. Pri razvrščanju predlogov so odločilne predvsem preteče nevarnosti in slabosti. Pri prvi organizaciji (preglednica 9) najbolje uvrščeni predlogi vrzeli po oceni precej odstopajo. Naslednji štirje so prejeli enako število točk, vsi ostali pa so bili slabše ocenjeni. V nadaljevanju so najprej predstavljene SWOT ocene prvih osmih predlogov vrzeli iz preglednice 9.

Splošna analiza varnostnih vrzeli IS (2. org.)

Na seji možganske nevihte je zaposleni na servisu edini opozoril na zmotljivost, ki je lahko posledica pomote ali pa je njen vzrok v utrujenosti, če ne celo preobremenjenosti. Predlog je kot tretjega tudi uvrstil med ocenjevane, ocena kriterija pa je precej nizka (ocena 2). Na to vrzel vpliva poleg prej naštetih vzrokov še veliko drugih, ki jih je težko istočasno nadzorovati. Opisani predlog prav gotovo ni nepomemben. Zmota pri nastavitvi pravilne konfiguracije varnostnih elementov ima lahko za organizacijo katastrofalni učinek. Zato je še kako pomembno, da zaposleni pri izvedbi projektov delujejo proaktivno in sproti rešujejo probleme na postavljenih nalogah. Če se ti kopičijo, lahko pride do preobremenjenosti, ko se bližajo roki izvedbe. Sledi utrujenost in takoj veliko večja verjetnost, da pride do napak. V stolpcu 5-7 intuitivno izbranih predlogov iz preglednice 10 sta le dva ocenjevalca navedla vseh sedem predlogov. Vsi ostali so izpolnili le po pet predlogov. Tako kot pri raziskavi v prvi organizaciji smo se odločili, da večjo pozornost namenimo osmim najbolje ocenjenim predlogom vrzeli v preglednici 12. V nadaljevanju so predstavljene njihove SWOT ocene.

Analiza SWOT varnostnih vrzeli IS (1. org.)

Presojamo predvsem slabosti, priložnosti in možne nevarnosti. Na sliki 6 je primer takšne analize za predlog vrzeli, ki mu je ocenjevalna skupina prve organizacije pripisala največji pomen in mu dodelila največje število točk. Analiza preostalih predlogov vrzeli je v prilogi 5.

S (Prednosti /Strengths/) ● potrebno je manjše število ERP licenc (ugodnejše s finančnega vidika); ● zamenljivost uporabnikov (prerazporejanje); ● manjši stroški šolanja; ● izogib zamudnemu dodajanju in odvzemanju rol s strani sistemskega inženirja; ● delo z isto licenco v dopoldanski in popoldanski izmeni.	**W (**Slabosti /Weaknesses/) ● otežena presojna sled na sistemu (kdo, kdaj, kaj) v primeru da ni vključenega sledenja na bazi (auditing); ● večja verjetnost napak na finančnih, planskih in ostalih podatkih; ● možen nepooblaščen dostop do ostalih modulov ERP sistema; ● nepooblaščeno izvajanje kalkulacij na planskih podatkih negativno vpliva na storilnost sistema; ● večje tveganje z vidika varnosti.
O (Priložnosti /Opportunities/) ● ponudba licenc pogodbenega partnerja pod ugodnejšimi pogoji; ● promocijska ponudba šolanj ERP sistema s strani pogodbenega partnerja; ● prihod ugodnejšega ponudnika ERP sistema na notranji trg; ● ugodnejša davčna zakonodaja na področju vlaganj v posodobitev poslovanja.	**T (**Nevarnosti /Threats/) ● zavračanje faktur s strani kupcev ali dobaviteljev; ● zmanjšanje naročil kupcev; ● negativni vpliv na ugled organizacije; ● zaostritev pogojev OEM sodelovanja s strani naročnika.

Slika 6: **Analiza SWOT predloga vrzeli dostopa do ERP sistema**

Kazalniki SWOT matrike

prednosti:

- število prihranjenih ERP licenc/modul;
- zamenljivost števila uporabnikov/izmeno;
- stroški šolanja v EUR/polletje;
- število spremenjenih rol/modul.

slabosti:

- število napak v podatkih/modul;
- število dostopov/modul;
- poraba CPU časa sistema/modul;
- število varnostnih incidentov ERP sistema/polletje.

priložnosti:

- število kupljenih licenc/posebno ponudbo;
- število šolanj/posebno ponudbo;
- število novih ERP ponudnikov/leto;
- število davčnih vzpodbud/leto.

nevarnosti:

- število zavrnjenih faktur/polletje;
- število naročil/polletje;
- število kritik v medijih/polletje.

Štirje od sedmih ocenjevalcev (57 %) so ta predlog upoštevali v svoji ožji oceni. Če ni vključena sledljivost baze podatkov, zaradi česar programska rešitev deluje hitreje, je ob nedosledni evidenci kasneje težko ugotavljati, kdo in kje je spreminjal podatke na bazi. Na seji iskanja vrzeli IS je udeleženka s finančnega oddelka izpostavila ta predlog kot problem. Finančni modul je tisti, s katerim naj bi upravljali le dobro usposobljeni in izkušeni uporabniki. V preteklosti je v času nadomeščanj uporabnikov ali ob naslednji izmeni že prihajalo do pomot na finančnih podatkih ali fakturah. Če sta z isto licenco delala dva uporabnika, je težko dokazati, kateri je povzročil napako. Do namerne zlorabe ERP sistema kljub pomanjkanju števila licenc doslej ni prihajalo.

Analiza SWOT varnostnih vrzeli IS (2. org.)

Na spodnji sliki je primer, ki mu je ocenjevalna skupina v drugi organizaciji pripisala največji pomen in mu dodelila največje število točk. Analiza preostalih predlogov vrzeli je v prilogi 6.

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● dostopnost izven delovnega mesta; ● dostop do elektronske pošte; ● navigacija doma in v tujini do znanega cilja službene poti (GPS); ● 24/7 dosegljivost (klici, SMS, e-pošta).	● treba je paziti na baterijo, da je dovolj polna; ● različni vmesniki za priklop polnilnika v tujini (ZDA, Velika Britanija); ● uporabnik je pod nadzorom, kje se giblje (GSM cona); ● privzete nastavitve; ● slabša vidljivost zaslona na dotik na prostem (sonce); ● proženje storitve po pomoti ob dotiku napačne ikone na zaslonu.
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● novi modeli, z dodatnimi funkcijami, ki jih ponuja trg; ● aneksi k podaljšanju naročniških pogodb, ki omogočajo cenovno ugodno menjavo za novejše modele; ● večje število ponudnikov mobilnih storitev z možnostjo izbire najugodnejšega za podatkovni prenos; ● modeli 3. generacije tablic z Wi-Fi dostopom in možnostjo telefona.	● možnost kraje na javnih mestih; ● prestrezanje podatkov na brezžičnih javnih in brezplačnih omrežjih (hoteli, knjižnice, internetne kavarne itd.); ● izpostavljenost direktnemu soncu na delovnem mestu v času odsotnosti zaposlenega; ● razvoj virusne programske kode na tabličnih operacijskih sistemih; ● favoriziranje monopolnega ponudnika podatkovnega prenosa in internetnih storitev ter posledično višja cena.

Slika 7: Analiza SWOT predloga vrzeli pametni telefoni

Kazalniki SWOT matrike

prednosti:

- število prejetih službenih klicev izven delovnega časa/mesec;
- število prejetih službenih SMS sporočil izven delovnega časa/mesec;
- število prejetih službenih poštnih sporočil izven delovnega časa/mesec.

slabosti:
- število primerov potreb po vmesniku za polnjenje/leto;
- število pomot, ki so posledica zaslona na dotik/mesec.

priložnosti:
- število novih modelov istega ranga/leto;
- število izkoriščenih aneksov pogodb/leto;
- število novih ponudnikov mobilnih storitev/leto.

nevarnosti:
- število odtujitev naprav/leto;
- število novih primerov virusov/polletje.

Pametni telefoni (preglednica 12) so prejeli skoraj dvojno število točk kot predlogi 2, 3 in 4. Na ocenjevanju se je zanje odločilo šest od desetih (60 %) ocenjevalcev. Član skupine iz oddelka trženja je ta predlog sicer uvrstil med sedem intuitivno izbranih, ni ga pa dal v ožji izbor ocenjevanja. Večjo vlogo je pripisal kraji prenosnika z mediji USB, pravilni konfiguraciji varnostnih elementov in varnostnim kopijam podatkovne baze ERP sistema. Njegovo odločitev bi lahko razumeli, da je telefon zanj sicer pomemben, toda ne tako ogrožen vir. Vprašanje pa je, ali je imel v mislih dejstvo, da je preko telefona lahko ogrožen njihov IS. Ocenjujemo, da je pametni telefon za uspešno delo zaposlenih v oddelku trženja zelo pomemben informacijski vir. Uporaba zahteva spoštovanje vseh predpisanih varnostnih ukrepov, da z njim ne ogrozimo varnosti sistemov znotraj organizacije. Največje število točk je pametnim telefonom pripisal ocenjevalec oddelka OE rešitve.

Zaposleni iz sistemske administracije vidi pametne telefone kot precej pomembno varnostno vrzel. Predlog je uvrstil na prvo mesto tako pri intuitivni uvrstitvi sedmih predlogov kot pri treh predlogih, ki jih je ocenil. K odpravi te vrzeli bo lahko prispeval tudi sam s svojimi dosedanjimi tehničnimi izkušnjami in kompetencami na področju varnostnih elementov omrežja. Zaveda se tudi, kako pomembno je dnevno spremljanje posodobitev programske opreme varnostnih elementov in dodatkov, ki se z razvojem novih storitev stalno dopolnjujejo na strani ponudnikov.

Precej uglašeno sta ocenjevala oba člana iz oddelka izvedbenih rešitev. Predlog pametnih telefonov sta uvrstila na tretje mesto med ocenjenimi predlogi. Večjo težo sta pripisala strukturnemu kapitalu in natisnjenim dokumentom na tiskalniku. Na številne možnosti, ki jih imajo v organizaciji na področju strukturnega kapitala, smo skupino zaposlenih opozorili na prvem srečanju. Omenjena ocenjevalca sta temu predlogu dala precej visoki in celo popolnoma enaki oceni. Kot kaže, se zavedata, da se njihov oddelek lahko kmalu pridruži razvojnemu, ki trenutno možnost Wiki baze znanja največ uporablja.

Povzetek SWOT ocen (1. org.)

Na koncu priloge 5 smo napravili povzetek treh kriterijev SWOT ocene za osem obravnavanih vrzeli. Naša analiza ocenjenih vrzeli temelji predvsem na domnevnih nevarnostih in slabostih. Dobra polovica ocenjevalcev je menila, da je treba najti ustrezno rešitev varnejšega in odgovornejšega dostopa do ERP sistema. Težko je namreč najti presojno sled, če se z eno licenco lahko prijavljata dva uporabnika. Obstajati mora utemeljen razlog, da se odgovorni odločijo za snemanje (auditing[8]) aktivnosti na bazi podatkov. Sistem se medtem odziva počasneje, kar vpliva na storilnost zaposlenih na njem. Ukrep je namenjen raziskovanju napak v podatkih in temu, kdo je te podatke obdeloval, gre za ugotavljanje posledic. Med nevarnostmi smo omenili pomote na finančnih podatkih, ki so lahko posledica ravnanja neveščega, ne dovolj zbranega ali morda preobremenjenega uporabnika. Na osnovi ugotovitev ima moderator na seji iskanja rešitev možnost usmeriti skupino proti taki, ki bo učinkovito odpravila pomote, tj. vzroke napak. Glede na zahtevnost in pomen informacijskega vira je predlog upravičeno na prvem mestu za obravnavo na 2. srečanju skupine. Sledi primer dveh vrzeli, ki sta prejeli enako oceno. Pomen vrzeli arhivskih podatkov je za organizacijo nedvomno večji od pomena vrzeli VPN dostopa do notranjega omrežja organizacije. V primeru da bi se za arhiv v večjem obsegu uresničila ena izmed naštetih nevarnosti (požar, poplava), bi organizacija lahko ostala brez shranjenih podatkov v elektronski, papirni obliki ali obeh. To bi za nadaljnje poslovanje lahko imelo resne posledice. Razvrstitev obeh vrzeli za obravnavo na 2. srečanju ohranimo v obstoječem zaporedju. Hkrati upoštevamo mnenje ocenjevalcev, da so VPN dostopi do omrežja pomembnejši za hitro reševanje problemov oz. posodobitev ERP sistema s strani pogodbenega partnerja kot preostale vrzeli, ki sledijo in jih obravnavamo v nadaljevanju. Nadaljujemo z razvrščanjem štirih predlogov vrzeli z enako oceno. Na osnovi domnevnih nevarnosti ocenjujemo, da ima vrzel Nadomeščanja v času odsotnosti med njimi največjo težo. Še posebej to velja za osebje IT, ki skrbi za nemoteno delovanje ERP sistema in uporabnike finančnega modula. V primeru da je odsotna ključna oz. težko nadomestljiva oseba za delo na projektu, se njegov rok izvedbe podaljšuje. Ko tehtamo domnevne nevarnosti preostalih treh vrzeli, menimo, da je treba dati prednost reševanju neurejenega stanja osnovnih virov. Po eni strani nastaja neposredna škoda v evrih pri pripravi letnega proračuna za nakup novih osnovnih virov, pa tudi napačno prikazovanje stanja osnovnih virov v produkciji. To nadalje vpliva na nepravilno prikazovanje ocen na višjih ravneh, ki temeljijo na teh podatkih. Vrzeli Uganljivih gesel damo prednost pred Prenosnimi računalniki za privatne zadeve, ker je preko lahko uganljivega gesla mogoče zlorabiti tudi ERP dostop ali dostop do elektronske pošte. Povzetek razvrstitve vrzeli po SWOT oceni smo prikazali v drugem stolpcu preglednice 9.

Povzetek SWOT ocen (2. org.)

Na koncu priloge 6 smo napravili povzetek treh kriterijev SWOT ocene za osem obravnavanih vrzeli. Analiza ocenjenih vrzeli temelji predvsem na domnevnih nevarnostih in

[8] Nastavitev na podatkovni bazi, ki omogoča sledenje aktivnosti uporabnikov na njej.

slabostih. Pri oceni pametnih telefonov smo navedli nekaj slabosti, ki jih uporabnik hitro premaga z dnevno uporabo. Zaposleni, ki je pogosto na službeni poti, zagotovo vedno nosi v poslovnem kovčku vmesnik za polnilnik napajanja. Večini nevarnosti se uporabniki z doslednim upoštevanjem priročnika uporabe in varnostnih politik lahko izognejo. Vrzel je s strani ocenjevalcev prejela skoraj dvojno število točk v primerjavi s tremi vrzelmi, ki ji sledijo v preglednici 12. Pri iskanju rešitev zato zahteva še posebno pozornost. Sledijo tri vrzeli, ki so jih ocenjevalci enako ocenili. Najprej tehtamo med predvidenimi nevarnostmi. Te pri vrzeli Neustrezno nastavljenih varnostnih elementov omrežja s puščanjem možnosti zlorab na internem omrežju gotovo prevladajo nad nevarnostjo odtujitve prenosnika ali posameznih podatkov konkurenci. Uvrstitve te vrzeli zato ne spreminjamo. Naprej se odločamo o tem, kaj nam pomeni večjo izgubo: kraja prenosnika z nekaj uporabnikovimi podatki ali odhod visoko usposobljenega zaposlenega h konkurenci. Če je organizacija v preteklosti vanj še precej vlagala in bo z njim odšlo tudi znanje, bomo gotovo dali prednost vrzeli Strukturnega kapitala. Moderator ima na 2. srečanju možnost skupino usmeriti k rešitvi, ki naj bi učinkovito omogočala strukturiranje znanja takšnega zaposlenega še v času zaposlitve. Sledita ponovno dve enako ocenjeni vrzeli.

Menimo, da je nevarnost, da uporabniško ime in geslo ne prideta v roke nepooblaščenim večja od morebitnega stranskega učinka, ki ga povzroči ne dovolj preizkušeni popravek na programski opremi komunikacijskega elementa. Zato damo prednost Vrzeli Pridobitve uporabniškega imena in gesla. To pomeni spremembo dosedanje razvrstitve teh dveh vrzeli. Tudi pri naslednjih dveh vrzelih storimo podobno. Samodejni vklop vgrajenega sistema za gašenje predstavlja veliko večjo nevarnost za vso nameščeno aparaturno opremo v sistemskem prostoru kot npr. to, da nekdo na tiskalniku pozabi dokument, ki pride v roke drugemu zaposlenemu. Da bi prišel v roke obiskovalcu, je večinoma izključeno, ker ta ne more hoditi sam, brez spremljevalca, po organizaciji. Povzetek razvrstitve vrzeli po SWOT oceni smo prikazali v drugem stolpcu preglednice 12. Na drugem srečanju skupine se želimo osredotočiti na iskanje rešitev petih največjih ugotovljenih nevarnosti IS. Dobljena razvrstitev vrzeli bo v nadaljevanju upoštevana še pri preverjanju s tabelo ocene tveganja.

Analiza predlogov vrzeli obeh organizacij s tabelo ocene tveganja

Prvih osem, po SWOT oceni razvrščenih varnostnih vrzeli v obeh organizacijah, preverimo še skozi prizmo ocene tveganja. V ta namen uporabimo preglednico 1 na strani 15. Ta ocena nam omogoči, da še natančneje razvrstimo predloge, ki so na ocenjevanju prejeli enako število točk. Pri razvrščanju damo prednost tistim predlogom, ki v tabeli tveganja dosežejo večjo številčno vrednost. Večja vrednost pomeni, da varnostna vrzel predstavlja večje tveganje za informacijsko varnost. Rezultati preverjanja za prvo organizacijo so prikazani v preglednici 13, za drugo pa v preglednici 14.

Preglednica 13: Analiza predlogov vrzeli s tabelo ocene tveganja (1. org.)

Vrstni red predlogov vrzeli SWOT ocene		Vrstni red vrzeli po ocenjevanju s tabelo	Število dobljenih točk iz ocenjevanja	Ime predloga za ranljivost IS	Stopnja grožnje	Stopnja ranljivosti	Vrednost vira	Številčna vrednost iz tabele ocene tveganja
1	*	1	17	Dostop do ERP sistema (kalkulacije, planski podatki)	V	V	V	7
2		2	13	Neurejen arhiv (poplavno področje tovarne)	V	S	V	6
3		3	13	VPN dostopi do omrežja organizacije	V	S	S	5
4		4	5	Nadomeščanje v času odsotnosti	S	S	V	5
5		7	5	Osnovni viri (evidence, stanje na terenu, reverzi)	N	S	M	2
6		5	5	Uganljiva standardna gesla	V	S	S	5
7		6	5	Uporaba prenosnikov za privatne zadeve (certifikati)	V	S	S	5
8		8	4	Izklapljanje delovnih postaj	N	N	M	1

N – nizka; S – srednja; M – majhna; V – visoka.
* Poudarjeno so označene izbrane vrzeli za obravnavo v Fazi 3 (2. srečanje skupine).

Argumenti ocenjevanja tveganja v preglednici 13 (1. org.)

1: Grožnja odpovedi sistema je velika. Zaradi premajhnega števila licenc je sistem zelo ranljiv. ERP sistem predstavlja za organizacijo veliko vrednost.

2: Dosedanji veljavni pravilnik (varnostna politika organizacije) je dovoljeval izgubo podatkov IS za največ en delovni dan. Temu je sledil tudi DRP postopek varnostnega kopiranja, v primeru da bi prišlo do incidenta katastrofalnih razsežnosti. Zaradi bližine reke je grožnja velika, stopnja ranljivosti pa je glede na dosedanje pozitivne izkušnje srednja. Vrednost vira je za organizacijo velika (zakonsko predpisan papirni arhiv, dnevne in arhivske kopije IS).

3: Grožnja nepooblaščenega dostopa je velika. Uporabniki, ki ta dostop imajo, spadajo med napredne in ozaveščene. Stopnja ranljivosti je zato srednja. Cena oz. vrednost vira, če jo primerjamo z ostalimi sistemi, je srednja.

4: Grožnja nepooblaščenih dostopov med nadomeščanjem pa tudi sicer je srednja (primer: izvajanje kalkulacij planskih podatkov). Doslej ni bilo zlorab, zato ranljivosti damo srednjo oceno. Nadomeščanje, predvsem v IT oddelku in financah na ERP sistemu, ima veliko vrednost.

5: Stopnja grožnje za evidence trenutnega stanja osnovnih virov je nizka. Ranljivost, da do razhajanja med obema evidencama pride, je srednja Vrednostna ocena razhajanja med stanjem osnovnih virov na terenu in v evidencah je majhna.

6: Grožnja nepooblaščenih dostopov je velika (enostavna, uganljiva gesla). Doslej zlorab ni bilo (posojanje prijavnega imena), zato je ranljivost srednja. Vrednost je srednja (event. administracija gesel).

7: Grožnja, da se na odtujenem prenosniku pridobi instalirani certifikat, je velika. Glede na dosedanje pozitivne izkušnje je ranljivost srednja. Sorazmerno zmogljivi prenosni računalniki (z izjemo tistih iz razvoja) so danes dosegljivi za sprejemljivo ceno, zato je vrednost vira srednja.

8: Vključena delovna postaja sicer ne predstavlja posebne varnostne grožnje, je pa energijsko gledano neracionalna, še posebej, če je število vključenih postaj v celotni organizaciji veliko. Gre za delovne postaje znotraj organizacije, zato je stopnja ranljivosti nizka. Vrednost tako porabljene energije v primerjavi s stroji v proizvodnji je majhna.

Preglednica 14: Analiza predlogov vrzeli s tabelo ocene tveganja (2. org.)

Vrstni red predlogov vrzeli SWOT ocene		Vrstni red vrzeli po ocenjevanju s tabelo	Število dobljenih točk iz ocenjevanja	Ime predloga za ranljivost IS	Stopnja grožnje	Stopnja ranljivosti	Vrednost vira	Številčna vrednost iz tabele ocene tveganja
1	*	1	22	Pametni telefoni	S	V	V	6
2		2	12	Pravilna konfiguracija varnostnih elementov omrežja	V	S	V	6
3		3	12	Strukturni kapital	V	N	V	5
4		4	12	Kraja prenosnika, medijev USB itd.	S	S	S	4
5		5	9	Pridobitev uporabniškega imena in gesla	N	S	V	4
6		6	9	Spremljanje vrzeli na komunikacijski opremi	N	S	V	4
7		7	8	Sistemski prostor (sistem zavarovanja)	V	N	S	4
8		8	8	Natisnjeni dokumenti na tiskalniku	N	S	S	3

N – nizka; S – srednja; V – visoka.

* Poudarjeno so označene izbrane vrzeli za obravnavo v Fazi 3 (2. srečanje skupine).

Argumenti ocenjevanja tveganja v preglednici 14 (2. org.)

1: Stopnja grožnje upošteva, da so uporabniki napredni in ozaveščeni, zato je srednja. Ranljivost vira je velika (kraja na javnem mestu, v hotelu). Cene telefonov so visoke. Vrednost upošteva tudi morda izgubljene podatke.

2: Grožnja zaradi nepravilnih nastavitev je velika. Opravka imamo z virom, katerega nepravilno delovanje ali odprtost zaradi nepravilnih nastavitev predstavlja veliko grožnjo za

IS organizacije. Ponudniki se velikokrat odločajo za svoje programske rešitve na najnižjem nivoju upravljanja. Dokumentacija o njih je skopa ali je sploh ni, zato tudi hekerji tem napravam teže pridejo do živega. Stopnji ranljivosti smo zato dali srednjo oceno. Ta oprema je specialna, zato je vrednost vira za organizacijo velika.

3: Stopnja grožnje (npr. odhoda znanja iz organizacije) je velika. Ranljivost vira je nizka, ker ti dogodki niso tako pogosti. Vrednost vira je velika in pomembna za organizacijo, če vodilni zaposleni v njej to spoznajo. Govorimo o znanju in izkušnjah, ki se iz glav zaposlenih preselijo v strukturirano obliko Wiki baze na internem komunikacijskem sistemu. Z ustrezno konfiguracijo in omejitvami dostopa posameznih delov pooblaščenim skupinam lahko tveganje zlorabe teh podatkov (tudi s strani zaposlenih) precej zmanjšamo. S tem se avtomatično zmanjša tudi ranljivost. S strukturnim kapitalom se organizacija lahko zavaruje pred odhodom znanja iz nje, ko jo zapusti nekdo od zaposlenih s pomembne funkcije (odpoved delovnega razmerja, daljša bolniška odsotnost, smrt itd.). Na sliki 10 smo opozorili posledično tudi na povečanje tržne vrednosti organizacije.

4: Grožnja odtujitve in stopnja ranljivosti je srednja, ker so uporabniki napredni in ozaveščeni in imajo ponavadi diske zaščitene s kodo (inkripcijo). Vrednost prenosnika je srednja.

5: Grožnja je nizka, primeri so izredno redki. Ranljivost v zvezi s tem obstaja na srednji ravni. Če je zlorabljeno zaupanje, je vrednost za organizacijo velika, saj ta gradi namreč na zaupanju.

6: Grožnja morebitne odkrite vrzeli na programski opremi komunikacijskih naprav je nizka, ker se to dogaja redkeje. Gre za zelo profesionalno opremo znanih proizvajalcev, zato je ranljivost srednja. Prav zaradi profesionalne opreme je ta draga in predstavlja za organizacijo veliko vrednost.

7: Grožnja, ki jo predstavlja aktiviranje varnostnega sistema zavarovanja, je velika. Tovrstna zaščita se izpopolnjuje in se to izredno redko zgodi, zato je ranljivost nizka, za organizacijo pa predstavlja ta vir srednjo vrednost.

8: Stopnja grožnje pozabljenega dokumenta na tiskalniku je nizka. Dogaja se redkeje (ob zastoju papirja v tiskalniku, napaki pri tiskanju ipd.), zato je ranljivost srednja. Vrednost je odvisna od vsebine dokumenta. Ocenili smo jo s srednjo. Verjamemo, da se dokumenti zaupne narave tiskajo previdneje.

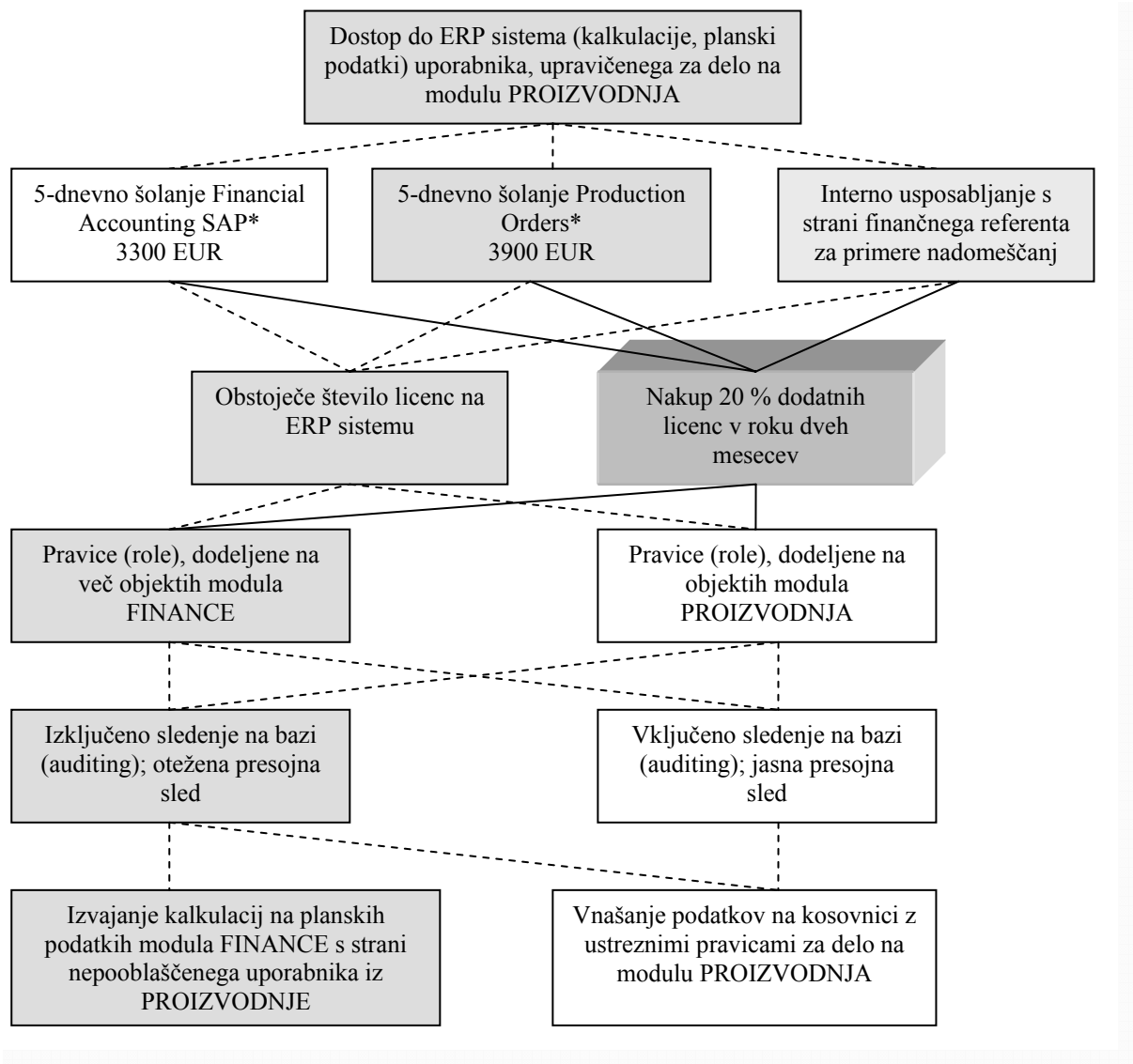
Povzetek ocenjevanja tveganja v obeh organizacijah

Za prvo organizacijo ocena najbolje uvrščenih dveh vrzeli kaže, da upravičeno zaslužita prednostno obravnavo na 2. srečanju skupine. VPN dostopu do omrežja zaradi višje stopnje grožnje damo prednost pred vrzeljo Nadomeščanja v času odsotnosti kljub enaki skupni oceni

tveganja. Večje tveganje za informacijsko varnost predstavljata tudi vrzeli Uporabe prenosnikov in Uganljivih gesel v primerjavi z bolje uvrščenimi Osnovnimi viri. Iz enakega razloga kot pri SWOT ocenjevanju damo prednost Uganljivim geslom. Ocenjevanje s tabelo kaže najmanjše tveganje za vrzel Izklapljanja delovnih postaj, zato je vrzel Osnovnih virov uvrščena za mesto višje.

Tudi pri drugi organizaciji najbolje uvrščeni vrzeli zahtevata prednostno obravnavo pri iskanju možnih rešitev. Ocenjevalna skupina se je dobro zavedala pomena strukturiranja znanja zaposlenih. Ocena tveganja Strukturnega kapitala opozarja na to, da je glede na konkurenčno okolje na trgu grožnja po odhodu boljših, če ne najboljših kadrov h konkurenci, velika. V take kadre organizacija veliko vlaga z namenom, da s proizvodi in storitvami lahko sledi trendom na tržišču. Sledijo štiri vrzeli z enako oceno tveganja. Pri razvrstitvi upoštevamo tudi oceno ocenjevalne skupine. Zato je kot četrta Kraja prenosnika in medijev USB. Peta in šesta vrzel imata po SWOT ocenjevanju enako oceno skupine in stopnjo tveganja. Iz istega razloga kot pri SWOT oceni tudi tu damo prednost vrzeli Pridobitve uporabniškega imena in gesla. Zadnji dve vrzeli imata enako oceno pomembnosti, ocena tveganja pa ju uvršča tako kot predhodna SWOT ocena. Ugotovimo lahko, da se vrstni red vrzeli v preglednici 14 po tej izbiri ni spremenil.
Tri najbolje ocenjene predloge varnostnih vrzeli, dobljene s pomočjo obeh metod, analiziramo še s finančne plati. Ena od možnosti za takšno oceno je Schneierjeva metoda drevesa napada. Strošek, ki ga odkrita varnostna vrzel lahko povzroči v primeru da pride do njene zlorabe, je dodatno merilo uvrstitve vrzeli po pomembnosti za njeno obravnavo na 2. srečanju. V nadaljevanju so prikazane ocene treh najbolje ocenjenih vrzeli iz obeh organizacij s Schneierjevo metodo drevesa napada.

Analiza vrzeli obeh organizacij s Schneierjevim diagramom drevesa napada



* Http://www.sap.com/slovenia/services/education/pdf/2011_Course_Schedule_SAPSLO.pdf (21. 4. 2012).
--- Možno; — Ni možno.

Slika 8: Schneierjev diagram nepooblaščenega dostopa na ERP sistemu (1. org.)

Za primer vzamemo, da je uporabnik iz oddelka proizvodnje obiskoval petdnevni tečaj naročanja materiala za delo na proizvodnem modulu ERP sistema. Zaradi premajhnega števila licenc uporablja prijavo, ki so ji na bazi podatkov dodeljene poleg proizvodnega tudi pravice do več objektov finančnega modula. Vodja sistemske administracije je na seji omenil, da razmišljajo o dokupu licenc. Trenutno stanje temu uporabniku dovoljuje, da lahko izvaja kalkulacije na planskih podatkih finančnega modula. Znanje o tem je pridobil bodisi na internem usposabljanju s strani enega od referentov finančne službe bodisi sam s pomočjo uporabniške dokumentacije. Sledljivost na bazi (auditing) je na sistemu vključena le izjemoma. V primeru da je izključena, nadzor ni mogoč nad nepooblaščenim dostopom do

planskih podatkov s strani nepooblaščenega uporabnika, ki sicer dela na proizvodnem modulu. Za delo na finančnih podatkih je morda upravičen le za čas nadomeščanja v izjemnih primerih. V primeru, ki ga je izpostavila skupina na prvem in drugem srečanju, se moramo predvsem vprašati po motivu uporabnika. V podpoglavju o varnostnih grožnjah smo opozorili, da gre lahko za nezadovoljnega ali nepoštenega zaposlenega. Morda se pripravlja na odpoved delovnega razmerja in tovrstne podatke želi uporabiti v novem okolju. Organizacija s tem izgubi šolanega uporabnika ERP sistema. Koliko so vredni odneseni podatki, lahko pokaže šele kasnejša analiza, če se ugotovi, za katere gre. Kot je razvidno iz slike 8, celotedenska izobraževanja predstavljajo precejšen strošek za organizacijo. Ta se ponovi, če je potrebno za delo usposobiti novega človeka, razen če so ta znanja postavljena kot pogoj za novo zaposlitev. Pri nepooblaščenem brskanju po planskih podatkih lahko pride tudi do njihove spremembe. Vprašanje je, kdaj se to opazi. Glede na to da sledenje na bazi ni vključeno, presojne sledi ni. Nastalo škodo predstavlja dodatno porabljeni čas finančnega referenta za iskanje in popravljanje spremenjenih planskih podatkov.

Neurejeni arhiv (1. org.)

Temu predlogu so največji pomen pripisali zaposleni iz kakovosti, financ in prodaje. Predstavnik kakovosti je dal kriteriju pomembnosti te vrzeli najvišjo oceno. Glede na področje, s katerim se ukvarja, in glede na izkušnje z dolgoletnim delom v organizaciji, ima njegova ocena še posebno težo. V prilogi 10 je prikazan možen scenarij zalitja prostora, v katerem se nahaja arhiv podatkov v papirni obliki, z vodo. Tovarna leži na poplavnem območju, v neposredni bližini reke. Poleg bližine reke smo v oceni SWOT omenili tudi požarno ogroženost. Še posebej velja to za papirna gradiva. Papirno gradivo, ki je hranjeno v namenskih protipožarnih in vodotesnih omarah, je v takem primeru sorazmerno na varnem. Enako velja za trakove zaščitnega kopiranja podatkov TSM[9] enote, če seveda ne gre za situacijo katastrofalnih razsežnosti. Vzeli smo primer, da se v prostoru arhiva na arhivskih regalih nahaja na novo prineseno papirno gradivo, ki je v fazi urejanja za arhiv in zlaganja v namenske omare. V primeru da je razsežnost poplave taka, da je voda vdrla v prostor in v njem stoji, obstaja velika nevarnost, da se papirno gradivo, ki je na regalih, navlaži. Če vzamemo prej omenjene katastrofalne razsežnosti, potem je tako papirno gradivo verjetno uničeno. Škodo se za tak primer lahko oceni šele, ko je znano, za katero papirno gradivo je natanko šlo. Enako velja za morebiti poškodovane TSM trakove.

VPN dostopi do omrežja (1. org.)

Pri intuitivni izbiri petih do sedmih predlogov so temu predlogu dali poudarek štirje ocenjevalci. Samo trije (43 %) pa so ga uvrstili med tri predloge, ki so jih ocenjevali. Možnost prijave na interno omrežje organizacije preko VPN kanala, je bila dana ob uvedbi ERP sistema. Namenjena je bila zunanjim vzdrževalcem in svetovalcem tega sistema po pogodbi.

[9]TSM – angl: Tivoli Storage Manager.

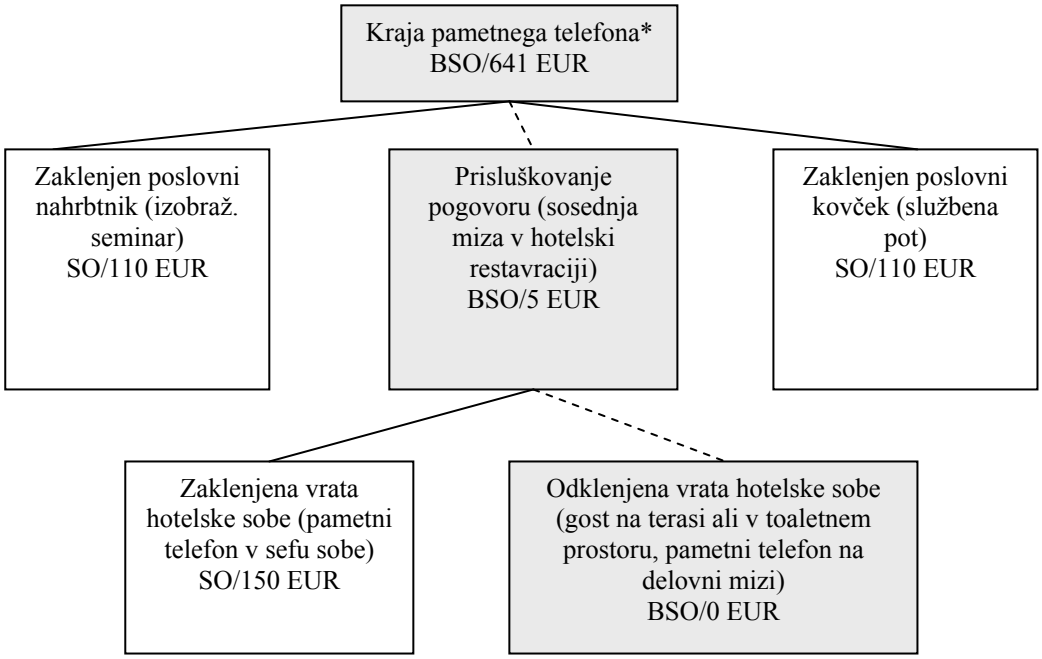
Vsak tak uporabnik se je moral v organizaciji najaviti, preden mu je bil ta dostop omogočen. Način prijave je priročen tudi za naprednejše uporabnike v organizaciji in razvojne inženirje, ki si svoje prenosne računalnike odnašajo domov. Dobre ideje in rešitve ne nastajajo le med službenim časom. Lahko se enemu od njih doma utrne zanimiva misel ali ideja in želi za njeno potrditev ali nadgradnjo podatke iz baznega oz. datotečnega strežnika internega komunikacijskega sistema. Morda doma preprosto nadaljuje z začetim delom v službi, ker mora biti projekt naslednji dan končan. Če gre za notranje uporabnike, najava v organizaciji pred dostopanjem ni potrebna.

V prilogi 11 je prikaz scenarija, ko je še neznani virus z interneta prenesenega programa okužil prenosnik razvojnega inženirja. Prisotnosti virusa še ne opazi, ker ga njegov protivirusni program ne zazna. Prijavi se preko VPN na interno omrežje in kopira omenjeni instalacijski program na skupno mapo strežnika v organizaciji. Ko začne z instalacijo na strežniku, izvršljiva instalacijska datoteka okuži tudi ostale datoteke skupne mape ali celo zagonski sektor na disku. Do skupnih map imajo dostop ostali uporabniki. Okuženo datoteko si tako ob prvem dostopu do nje prenesejo na svojo lokalno delovno postajo. Virus se nato širi naprej po organizaciji. O njem so preko spletnih forumov kmalu obveščeni. Škodo, ki je nastala, s prijavo zaposlenega razvijalca iz organizacije, se lahko oceni šele, ko je znano število okuženih delovnih postaj in strežnikov. Odstranjevanje virusov je lahko zamuden postopek in medtem na okuženih delovnih postajah ni možno delati ničesar. Še posebej neprijetno je, če se okuži zagonski sektor na diskovni enoti. V tem primeru se ne naloži operacijski sistem. Če so na postajah potrebne sveže instalacije operacijskega sistema, je škoda lahko zelo velika. Po končani instalaciji je namreč uporabnikom šele omogočeno, da si restavrirajo preostale delovne datoteke in programe ter ponovno vzpostavijo svoje prvotno delovno okolje.

V našem primeru smo vrednostno analizo s Schneierjevo metodo izpeljali za tri največje ugotovljene nevarnosti IS. Izvajalec metode se lahko odloči tudi drugače. Enako velja za ocenjevanje s tabelo tveganja. Ocena ni spremenila razvrstitve izbranih vrzeli za obravnavo v Fazi 3. Ni izključeno, da kakšna vrzel dobi prednost pri reševanju prav na osnovi rezultata Schneierjeve ocene. Z vrednostnimi ocenami dobi moderator dodatni pogled na vrzeli, ki so izbrane za 2. srečanje, kar mu koristi pri zastavljanju vprašanj in usmerjanju skupine, ki išče rešitve.

Pametni telefoni (2. org.)

Spodnja slika prikazuje možnost kraje pametnega telefona, ki je med predlogi varnostnih vrzeli najviše uvrščen. Najcenejša kraja, označena črtkano, ne zahteva nobene posebne opreme, zato je tudi najbolj verjetna.



BSO – brez specialne opreme.
SO – potrebna specialna oprema.
EUR – cena napada (kraje).
* Primer za Samsung Galaxy TAB 10.1; spletna cena brez naročniškega razmerja: 521 EUR**.
** Http://www.mobitel.si/telefoni-in-naprave/aparati.aspx?mo=0&te=0 (8. 4. 2012).
--- Možno; — Ni možno.

Slika 9: Schneierjev diagram možne kraje pametnega telefona (2. org.)

Nesporno je, da bodo te naprave sčasoma nadomestile prenosne računalnike. Še posebej imamo v mislih zaposlene iz oddelka trženja in prodaje. Razvojniki bodo še naprej bolj uporabljali prenosne računalnike, ki so robustnejši in v tem pogledu manj ranljivi. Pri delu predvsem programerji potrebujejo višjo procesorsko moč, da lahko hitro prevedejo in simulirajo delovanje razvite programske kode.

Tablični pametni telefon na službeni poti lahko nadomesti prenosni računalnik. Je prikladnejši in lažji od prenosnega računalnika. Če vzamemo za primer model, ki ga omenjamo v Schneierjevem diagramu na sliki 9, gre za velikostni razred, po dolžini in širini le dobro šestino manjši od lista papirja, formata A4 (pribl. 257 x 175 mm in debeline manj kot 9 mm). Mogoče ga je nositi v službeni torbi, večji ženski torbici, poslovnem nahrbtniku ali kovčku itd. Z njim je mogoče telefonirati, pošiljati SMS sporočila, brskati po internetu in upravljati s

službeno elektronsko pošto preko varne VPN povezave (z uporabo geselnika za prijavo). Omogoča nam urejanje besedila, preglednice, predstavitve predavanja ali ogled PDF dokumentov. Ima do osemkrat več delovnega spomina kot običajni prenosni računalniki. Operacijski sistem z namiznimi ikonami je na voljo takoj, brez čakanja (zagona sistema). Vgrajeni HD[10] snemalnik nam omogoča preslikavo dokumentov in njihovo takojšnjo uporabo v elektronski obliki. Ni vrtljivih delov, kot je primer diskovne enote prenosnega računalnika. To pomeni manjšo porabo energije in več dni avtonomije brez omrežnega napajanja. Vse našteto govori v prid dejstvu, da bo teh naprav v uporabi vedno več, kar hkrati ne pomeni tudi večje informacijske varnosti, prej večje tveganje. Varnost bo velika prav toliko, kolikor se bodo organizacije s svojo IT infrastrukturo in zaposleni temu prilagodili. Predvsem uporabniki bodo za varnost lahko napravili največ. To pa je dosledno izvajanje zastavljene in sprejete varnostne politike s strani vodstva organizacije in službe za informatiko.

Verjetnost, da tako napravo kje pozabimo, je precej večja kot pri prenosniku. Pri slednjem smo vajeni posebne torbe z napajalnikom in zunanjo miško za hitrejše delo. Običajno ga tudi ne nosimo vedno s seboj, pametni telefon pa bomo nosili že zaradi dostopnosti, imeli ga bomo večinoma pri sebi.

Ekspert in guru s področja informacijske varnosti Bruce Schneier je avtor t. i. metode drevesa napada. V osnovi gre za diagram poteka z vrha navzdol in na več ravneh scenarijev možnih situacij (v našem primeru kraje) za posamezni informacijski vir. Na sliki 9 je prikazano nekaj takšnih, ki so lahko povod za krajo pametnega telefona. Pri vsaki možnosti imamo v mislih protiukrep za dogodek in koliko nas ta stane v evrih. Dodamo tudi možnost v primeru da storilec potrebuje uporabo posebne opreme. Večinoma si prizadeva, da izpelje krajo s kar najmanj napora, hitro in brez večjega tveganja. Če obstaja priložnost, za katero ne potrebuje nobene posebne opreme, je ta po navadi najbolj verjetna, zato je ne smemo podcenjevati. Vrednost obravnavanega vira smo ocenili v spletni prodajalni enega izmed ponudnikov telefonskih storitev. Upoštevali smo nakup telefona v prosti prodaji, brez sklenitve naročniškega razmerja. Tej ceni smo prišteli približno mesečno zavarovanje telefona pri zavarovalnici proti kraji. Spletna cena aparata je 521 EUR, zavarovanje smo ocenili na 10 EUR/mesec, na letni ravni torej 120 EUR. Vir je za nas vreden 641 EUR. Telefon v uporabi, s kontaktnimi naslovi in podatki, je seveda vreden precej več. Upoštevati moramo izgubljeni čas nabavne službe ali tajništva, ki ga po odtujitvi porabi za nakup novega. V primeru da gre za naročniško razmerje, je tu še čas preklica stare številke in naročilo nove. Dodati moramo tudi čas uporabnika, preden ponovno vzpostavi okolje na njem za normalno delo (obnovitev kontaktnih telefonskih številk v imeniku, instalacija dodatne programske opreme za elektronsko pošto ali VPN odjemalca za varen dostop do omrežja organizacije itd.).

Vrednosti prvega in drugega nivoja diagrama v evrih so približne ocene. Če razpolagamo z natančnejšimi, jih navedemo. Organizacija se npr. odloči, da bo imetnikom pametnih telefonov kupila poslovne nahrbtnike, ki imajo vgrajeno ključavnico. Na spletnem naslovu znanega ponudnika tovrstne dodatne opreme najdemo tak nahrbtnik za ceno 110 EUR. V

[10] HD – angl: High Density.

organizaciji se dogovorijo, da se pametni telefoni na službeni poti na prostem nosijo izključno na rami, v zaklenjenem nahrbtniku. Za krajo pametnega telefona iz nahrbtnika bi tako storilec potreboval posebno opremo. V primeru da obstaja lažja varianta, se za to možnost verjetno ne bo odločil. V hotelu, ko so recimo zaposleni v bazenu, savni ali na večerji, naj bi bil takšen telefon raje v zaklenjenem sefu sobe ali na recepciji, nikakor pa ne na delovni mizici hotelske sobe ali nočni omarici. Pozabljena odklenjena vrata sobe so dovolj za storilca, da pride do našega telefona za nekaj evrov, saj je morda v restavraciji ali baru celo sledil našemu pogovoru s prijateljem ali poslovnim partnerjem in iz pogovora razbral številko naše sobe in lastništvo takšnega telefona. Tej situaciji smo dodelili simboličnih 5 EUR. Če se prej zapisanega zavedamo, bomo za pogovore raje izbirali diskretnejši prostor, kot sta kavarna ali bar.

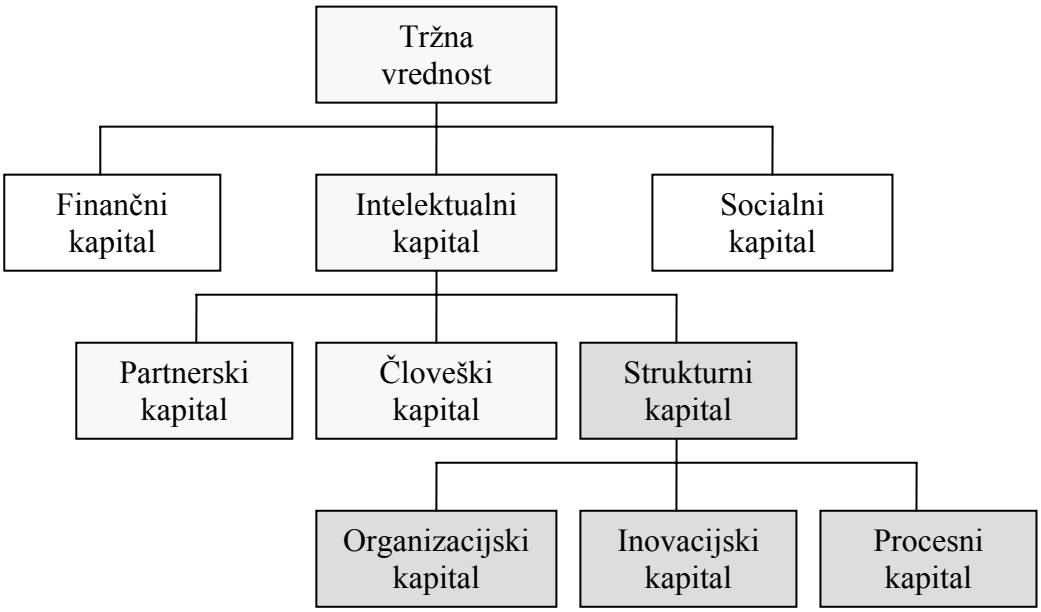
Na sliki 9 je označeno, katero možnost bi storilec za krajo najverjetneje izbral. Pri tem ne potrebuje nobene specialne opreme, kar bi ga sicer lahko ustavilo pri njegovi nameri. Številko hotelske sobe lahko storilec izve ob nepazljivem glasnem pogovoru v restavraciji hotela. V primeru da mu kraja uspe, dobi pametni telefon za vrednost zapitka v njej.

Pravilna konfiguracija varnostnih elementov omrežja (2. org.)

Varnostni elementi omrežja spadajo med specialno komunikacijsko opremo. Temu primerna je tudi cena te opreme in šolanja za njeno uporabo. V prilogi 8 je prikazanih nekaj teh možnosti. V diagramu je označena pot, ki jasno kaže, kdo naj bi posegal po nastavitvah teh elementov. Pravilno nastavljeni posamezni elementi so izrednega pomena za informacijsko varnost v organizaciji, zato naj bi bilo to prepuščeno res dobro izšolanemu kadru z opravljenimi mednarodno priznanimi certifikati. Tako izšolan kader je organizaciji potreben tudi, ko se to prijavlja na domače ali mednarodne razpise za pridobitev projektov. V izrednih razmerah, ko organizacija nima na razpolago svojega človeka, je najbolje, da prepusti to opravilo pooblaščenemu zunanjemu certificiranemu specialistu. Res je, da to ni poceni, a je škoda, ki lahko nastane ob nepravilnih nastavitvah, lahko neprimerno večja. Manjše organizacije, ki si težko privoščijo svoj kader za ta opravila, običajno najamejo zunanjega izvajalca, ki postavi in nastavi novo komunikacijsko opremo in skrbi za njene posodobitve.

Strukturni kapital (2. org.)

Intelektualni kapital ostaja še vedno dokaj odprta zgodba, ki nima dokončne rešitve. Strokovnjaki so se uspeli poenotiti le v tem, kaj intelektualni kapital sestavlja. Del tega je tudi strukturni kapital, ki se naprej deli na organizacijski, inovacijski in procesni, kot to prikazuje slika 10. Znanje, ki je bilo last posameznika, postane s tem kapitalom last organizacije in ima vpliv na njeno tržno vrednost.



Slika 10: Tržna vrednost in struktura kapitala

Vir: Lipparini 2002.

V organizaciji, ki je nosilec certifikata ISO 27001:2005, se dobro zavedajo, kako pomembno je znanje iz glav zaposlenih preseliti v strukturirano obliko, kar se trenutno največ izvaja v oddelku razvoja, kjer s pridom uporabljajo interno Wiki bazo, v katero pišejo posamezniki izkušnje in rešitve problemov, na katere so naleteli med svojim delom. Na tretjem srečanju je direktor poudaril, da ne gre pretiravati v smeri, da bi to vzelo zaposlenim preveč časa, vsi sogovorniki pa so se strinjali, da je strukturni kapital pomemben. V prilogi 9 smo skušali pokazati primer odhoda sistemskega administratorja iz organizacije v tujino. Želeli smo opozoriti, koliko stane organizacijo usposabljanje takšnega profila. V našem primeru je bil administrator v zahtevni vlogi tistega, ki lahko nastavlja varnostne elemente, med njimi tudi usmerjevalnike. V organizaciji bi kazalo razmisliti o tem, da bi tudi IT oddelek, podobno kot to že delajo v razvoju, gradil svojo Wiki bazo, ki bi bila z geslom dostopna le ožjemu krogu zaposlenih tega oddelka. Na ta način bi dosegli možnost nadomeščanja za primere bolezni ali daljše odsotnosti glavnega administratorja. V prikazanem scenariju bi lahko vsaj del znanja, dobljenega na večdnevnih specialnih šolanjih in certificiranju, po odhodu zaposlenega ostal v organizaciji. Vodja IT naj bi skupaj s svojimi ožjimi sodelavci, ki se lahko nadomeščajo, sestavil matriko podatkov, ki je bistvena za strukturiranje v njihovi Wiki bazi, predvsem pa morajo biti dobro dokumentirane vse trenutne in preizkušene nastavitve vitalnih delov varnostnih elementov in komunikacijske opreme. V primeru odpovedi je tako mogoče opremo nadomestiti z novo in jo nastaviti natanko tako, kot je bila prejšnja.

Spodnja preglednica kaže pet izbranih varnostnih vrzeli IS iz vsake organizacije, dobljenih kot rezultat prej prikazanega ocenjevanja in razvrščanja. V naslednji fazi se bo zanje iskalo najboljše možne rešitve.

Preglednica 15: Izbrane varnostne vrzeli predvidene za iskanje rešitev

Prva organizacija	Druga organizacija
Dostop do ERP sistema	Pametni telefoni
Neurejen arhiv	Pravilna konfiguracija varnostnih elementov omrežja
VPN dostopi do omrežja organizacije	Strukturni kapital
Nadomeščanje v času odsotnosti	Kraja prenosnika, medijev USB itd.
Uganljiva standardna gesla	Pridobitev uporabniškega imena in gesla

Faza 2B je s tem zaključena.

4.2.3 Faza 3 – iskanje in izbira rešitev varnostnih vrzeli IS

Prilagojena faza je sestavljena iz treh delov, in sicer 3A, 3B in 3C, kot je prikazano na sliki 5 na strani 21.

Faza 3A – iskanje rešitev varnostnih vrzeli IS (2. srečanje skupine)

Za varnostne vrzeli s seznama, sestavljenega v fazi 2B, smo z udeleženci skupine iskali konkretne in hkrati najbolj učinkovite možne rešitve zanje. Pri iskanju v prvi organizaciji so se sklicevali na pravilnik interne varnostne politike, nekateri udeleženci skupine v drugi pa na narejene ocene tveganja, ki so bile podlaga za pridobitev certifikata ISO 27001:2005. Na splošno morajo udeleženci pri izbiri rešitev upoštevati, da so te v skladu z internimi pravilniki, izdelanimi lastnimi rešitvami, veljavnimi standardi, priporočili dobrih praks, pa tudi kombinacijami med njimi. Cilj tega dela faze je bil najti in se uskladiti za rešitve petih izpostavljenih varnostnih vrzeli, ki so z vidika informacijske varnosti, v preglednici 13 za prvo in v preglednici 14 za drugo organizacijo, izbrane kot najpomembnejše, da se pristopi k njihovemu reševanju. S skupino je bilo na začetku dogovorjeno, da se med več predlaganimi rešitvami posamezne varnostne vrzeli za njeno najustreznejšo končno rešitev uskladi na samem srečanju. Delo s skupino je bilo na koncu tega dela faze zaključeno. Predlagane in končne rešitve udeležencev obeh skupin so predstavljene v nadaljevanju.

1.) Iskanje rešitev za predlog vrzeli "dostop do ERP sistema" (1. org.)

Komentar udeležencev med iskanjem rešitev:
Selektivno obvladovanje pravic na ERP sistemu je zelo zahtevno. Rešuje se z dodeljevanjem pravic uporabnikom s t. i. rolami. Teh je zelo veliko. Na delovnem mestu imajo uporabniki več zadolžitev (primer zaposlenih v nabavi oz. prodaji). Težko je recimo nekoga omejiti, da bo v določenem trenutku delal samo z naročilnicami, isti uporabnik je lahko zadolžen tudi za druga opravila. To bi pomenilo neprestano menjavanje pravic (rol) s strani sistemskega inženirja. Konfiguracija ERP prav tako ni enostavna (zasnovana je na objektih), da bi nastavljali pravila (npr. na nivoju transakcij). Nekdo ima lahko pravico dodajanja, drugi brisanja ali popravljanja, lahko pa tudi samo gledanja. Potrebe po sledljivosti (auditing) doslej ni bilo, ker ni znanih primerov zlorab. Prišlo je že do pomote, ne pa do zavestne zlorabe. Za dodeljevanje rol je trenutno odgovoren vodja službe za informatiko. V IT oddelku so štirje zaposleni (vodja IT, vodja sistemske administracije, aplikativni inženir za posebne programske rešitve in specialist za ERP sistem). Za pomoč uporabnikom so na razpolago vsi štirje preko sistema Helpdesk[11]. Uporabniki morajo napako obvezno prijaviti. Podporni sistem deluje zelo zanesljivo.

Predlogi rešitev vrzeli:
- še naprej je treba graditi na zaupanju in ozaveščenosti obstoječih in novih uporabnikov, ki imajo do te programske rešitve dostop;
- nakup dodatnih uporabniških licenc.

Končni predlog rešitve skupine za vrzel:
- še naprej je treba graditi na zaupanju in ozaveščenosti obstoječih in novih uporabnikov, ki imajo do te programske rešitve dostop.

2.) Iskanje rešitev za predlog vrzeli "neurejen arhiv" (1. org.)

Komentar udeležencev med iskanjem rešitev:
Predvsem gre tu za papirni arhiv. Magnetni trakovi TSM zaščitnega kopiranja so hranjeni na objektu. Podvojene lokacije hranjenja zaenkrat ni. Obstaja problem, ker se objekti držijo skupaj. Večjih potreb po restavriranju podatkov zaenkrat ni bilo. Zaščitno kopiranje je nastavljeno glede na naravo podatkov (dnevno kopiranje in inkrementalno). Zahteve za hranjenje arhivskega gradiva preko zunanjih ponudnikov tovrstnih storitev (Avtenta, Mikrocop, Pošta Slovenije, Mikrografija itd.) zaenkrat še ni bilo. (Primer: Hranjenje izdanih in prejetih faktur pri ponudniku). Vse izdane fakture so v PDF formatu, vse prejete fakture se optično preslikajo. Odločitev direktorja je, da hranjenje zagotovijo v organizaciji sami.

Predlogi rešitev vrzeli:
- hitra optična povezava do rezervne lokacije arhivskih podatkov;

[11] Programska oprema za prijavo napak.

- oddaja arhiviranja usposobljenemu zunanjemu ponudniku za hranjenje dokumentarnega in arhivskega gradiva.

Končni predlog rešitve skupine za vrzel:
- hitra optična povezava do rezervne lokacije arhivskih podatkov.

3.) Iskanje rešitev za predlog vrzeli "VPN dostopi do omrežja organizacije" (1. org.)

Komentar udeležencev med iskanjem rešitev:
Ta sistem priklopa je bil pol leta nazaj rezerviran (uporabljen) samo za zunanje izvajalce, tj. vzdrževalce in svetovalce ERP sistema preko vzdrževalne pogodbe. Dostop je sorazmerno odprt. Pred delom na daljavo se mora tak uporabnik najaviti (odvisno tudi od pomembnosti). Vsi uporabniki te storitve so profesionalni. Zaradi narave dela ima dostop tudi vedno več zaposlenih, ki delajo od doma, prav ti pa predstavljajo potencialno varnostno grožnjo.

Predlogi rešitev vrzeli:
- predlog je organizacijsko rešljiv v mesecu dni z nakupom novega VPN sistema. Dostop bo tako pod nadzorom v vsakem trenutku. Ta komunikacijska točka bo s tem v 90 % rešena, ker bo pod nadzorom. Podprta je možnost selektivnega dostopa do strežnikov. Po zapisih v log datotekah bo možno spremljati, koliko časa je bil kdo na omrežju, kaj je delal itd.;
- omejitev VPN dostopov.

Končni predlog rešitve skupine za vrzel:
- nakup novega VPN sistema.

4.) Iskanje rešitev za predlog vrzeli "uganljiva standardna gesla" (1. org.)

Komentar udeležencev med iskanjem rešitev:
V to kategorijo spadajo uporabniki Windows okolja, ki uporabljajo za geslo npr. le dve črki, kar že doslej ni standard v organizaciji in je prekršek varnostne politike.

Predlogi rešitev vrzeli:
- na sistemu je treba nastaviti avtomatizem, ki bo pri nastavitvi in menjavi gesla preveril, ali je geslo dovolj dobro (dolgo vsaj sedem znakov, med katerimi so tudi neabecedni znaki in številke), in ga šele nato dovolil uporabiti;
- periodično izvajanje nadzora in disciplinsko ukrepanje.

Končni predlog rešitve skupine za vrzel:
- na sistemu je potrebno nastaviti avtomatizem, ki bo pri nastavitvi in menjavi gesla preveril, ali je geslo dovolj dobro (dolgo vsaj sedem znakov, med katerimi so tudi neabecedni znaki in številke), in ga šele nato dovolil uporabiti.

5.) Iskanje rešitev za predlog vrzeli "nadomeščanje v času odsotnosti" (1. org.)

Komentar udeležencev med iskanjem rešitev:
Nadomeščanje specifičnega opravila, npr. finančne službe, se lahko izpelje po telefonu. Stvari se glede na vrsto problema rešujejo sproti. Polno nadomeščanje vodje IT in sistemskega inženirja ni pokrito. Doslej še ni bilo nobene negativne izkušnje, da bi to predstavljalo posebno ranljivost ali grožnjo. Določeno je tudi, da v obravnavani proizvodni organizaciji problem mora biti hitro rešen, ponavadi že preden bi se vzpostavila vsa potrebna pot reševanja.

Predlogi rešitev vrzeli:
- za problematiko IT je vedno vsaj 50 % zasedenost IT oddelka, kar pomeni stalno prisotnost vsaj dveh zaposlenih;
- postopno uvajanje nadomestljivega kadra za izredne razmere s pooblastilom;
- vzpostavitev baze znanja programske rešitve Helpdesk, ki bi veliko pripomogla k reševanju že znanih in že rešenih problemov (v stilu rešitev FAQ ipd.);
- možna je tudi specialna baza znanja (v obliki diagramov poteka določenih scenarijev opravil, ki so sicer delo sistemskega inženirja in specialistov), dostopna s posebnim geslom in evidenco dostopa do nje.

Končni predlog rešitve skupine za vrzel:
- za problematiko IT je vedno vsaj 50 % zasedenost IT oddelka, kar pomeni stalno prisotnost vsaj dveh zaposlenih.

Preglednica 16: Povzetek predlogov rešitev za izbrane vrzeli (1. org.)

Številka predloga →	1	2	3	4	5
Številka rešitve ↓	Dostop do ERP sistema	Neurejen arhiv	VPN dostopi	Uganljiva gesla	Nadomeščanje zaposlenih
1	Graditi na * zaupanju in ozaveščenosti obstoječih in novih uporabnikov	Hitra optična povezava do rezervne lokacije arhivskih podatkov	Nakup novega VPN sistema	Sistemska nastavitev kontrole kakovosti in periodične menjave gesel	Vedno 50 % zasedenost IT oddelka, stalna prisotnost vsaj dveh zaposlenih
2	Nakup dodatnih uporabniških licenc ERP sistema	Arhiviranje podatkov pri zunanjem ponudniku	Omejitev VPN dostopov	Periodično naključno izvajanje nadzora in disciplinsko ukrepanje	Uvajanje nadomestljivega kadra za izredne razmere
3					Vzpostavitev baze znanja programske rešitve Helpdesk
4					Spec. baza znanja v obliki diag. pot.

* Senčeno polje označuje končni predlog rešitve skupine za posamezno vrzel.

V preglednici 16 je prikazan povzetek vseh rešitev, ki jih je prispevala skupina za izbranih pet varnostnih vrzeli. Končni usklajeni predlogi so prikazani v senčenih poljih. Ker gre za prilagojeno fazo, je vsaka od predlaganih rešitev skupine naknadno ocenjena s strani avtorja magistrske naloge. Za ocenjevanje je uporabljena kvalitativna metoda KSF. Za dokončno izbiro (selekcijo) treh rešitev za vrzeli so upoštevani končni predlogi rešitve skupine in rezultati ocenjevanja (vrednost rešitve VR, izračunana s KSF oceno).

Po predhodno izbranih kriterijih in utežeh, ki so prikazani v preglednici 17, damo številčno oceno posameznemu kriteriju v vrednosti od 1 do 5. Kriteriji ocenjevanja so izvedljivost predlagane rešitve (K1), učinkovitost (K2) rešitve na informacijsko varnost v organizaciji in cena (K3) izvedbe oz. vpeljave rešitve. Vrednost 5 za kriterij izvedljivosti pomeni, da je rešitev izvedljiva takoj oz. zelo hitro, za učinkovitost, da je rešitev zelo učinkovita, za ceno pa, da rešitev ne predstavlja nobenega stroška. Kriteriju izvedljivosti smo dali prednost pred učinkovitostjo, zato mu je pripisana večja utež. Teoretično sicer lahko dobimo učinkovite

predloge rešitev za ranljivosti IS, ki pa so v praksi bodisi časovno, prostorsko in v končni fazi tudi cenovno težko izvedljivi.

Preglednica 17: Kriteriji in uteži ocenjevanja rešitev za uporabljeno metodo KSF

Kriterij	Opis kriterija	Utež (1-3)
K1	Izvedljivost	U1=3
K2	Učinkovitost	U2=2
K3	Cena	U3=1

K1, K2, K3 – ocenjevalni kriteriji za izvedljivost, učinkovitost in ceno.
U1, U2, U3 – vrednostne uteži za izvedljivost, učinkovitost in ceno.

Vir: Likar, Križaj in Fatur 2006, 84.

Preglednica 18: Ocenjevanje rešitev varnostnih vrzeli z metodo KSF (1. org.)

Številka predloga/rešitve	K1 Izvedljivost	U1	K2 Učinkovitost	U2	K3 Cena	U3	Vrednost rešitve (VR)
	1-5*	1-3	1-5*	1-3	1-5*	1-3	K1×U1+K2×U2+K3×U3
1 / 1	3	3	4	2	5	1	22
1 / 2	5	3	5	2	1	1	26
2 / 1	5	3	4	2	2	1	25
2 / 2	4	3	5	2	1	1	23
3 / 1	5	3	5	2	1	1	26
3 / 2	3	3	4	2	5	1	22
4 / 1	5	3	3	2	3	1	24
4 / 2	3	3	4	2	3	1	20
5 / 1	4	3	3	2	4	1	22
5 / 2	3	3	4	2	4	1	21
5 / 3	4	3	3	2	4	1	22
5 / 4	2	3	3	2	4	1	16

* Kriteriji K1, K2 in K3 se ocenjujejo z vrednostno oceno med 1 in 5, kot je prikazano spodaj.
K1 – izvedljivost: (5) izvedljivo takoj oz. zelo hitro, (4) izvedljivo z nekaj predhodne priprave, (3) izvedljivo na daljši rok, (2) izvedljivost je zadovoljiva, (1) ni izvedljivo.
K2 – učinkovitost: (5) zelo učinkovito, (4) dokaj učinkovito, (3) učinkovitost je dobra, (2) zadovoljiva učinkovitost, (1) neučinkovito.
K3 – cena: (5) stroškov ni, (4) strošek gre v rok službe, (3) cenovno ugodno, (2) sorazmerno visoka cena, (1) zelo visoka cena, drago.

Številčno vrednost posamezne rešitve (VR) dobimo z uporabo spodnje formule.

$$VR = K1 \times U1 + K2 \times U2 + K3 \times U3$$

Argumenti ocenjevanja kriterijev v preglednici 18 (1. org.)

1/1: zaupanje in ozaveščenost obstoječih in novih uporabnikov sta kategoriji, dosegljivi na daljši rok (K1=3). Ko se pri uporabnikih dosežeta, dokaj učinkovito vplivata na informacijsko varnost v organizaciji (K2=4). Stroškov s tem ni, potrebni sta le volja in želja, da se dosežeta (K3=5).

1/2: nakup licenc je mogoč takoj (K1=5). Zelo učinkovito pokrije odkrito varnostno vrzel ERP sistema (K2=5). Uporabniške licence so drage (K3=1).

2/1: hitra optična povezava do rezervne lokacije arhivskih podatkov je lahko hitro izvedljiva (K1=5). Problem vrzeli je s tem dokaj učinkovito rešen (K2=4), cena izvedbe je sorazmerno visoka (K3=2).

2/2: za arhiviranje pri zunanjemu ponudniku je nekaj več dogovarjanja in logistike, preden se vzpostavi (K1=4). Zelo učinkovito reši problem arhiviranja, saj ponudnik razpolaga z znanjem in sodobno opremo (K2=5), cena je visoka, se pa niža s številom tovrstnih ponudnikov na trgu (K3=1).

3/1: nakup novega VPN sistema je mogoč v kratkem času (K1=5). Zelo učinkovito odpravi varnostno vrzel (K2=5). Cena je visoka, saj gre za profesionalno opremo (K3=1).

3/2: omejitev VPN dostopov, če že, je treba izpeljati postopoma (K1=3). Dokaj učinkovito odpravi varnostno vrzel. Po uvedbi imajo dostop le zunanji vzdrževalci ERP sistema (K2=4). Ukrep ni povezan s posebnimi stroški (K3=5).

4/1: sistemska nastavitev kontrole kakovosti in periodične menjave gesel je mogoča v nekaj dneh (K1=5). Dobro rešuje problem varnosti dostopa do sistemov, toda traja kar nekaj časa, da jo uporabniki osvojijo in se je držijo (K2=3). Potrebna sta delo in nadzor sistemskega administratorja (K3=3).

4/2: periodično naključno izvajanje nadzora in disciplinsko ukrepanje je izvedljivo na daljši rok (K1=3). Dokaj učinkovito rešuje problem varnostne vrzeli (K2=4). Vključeno je delo izbranih zaposlenih, ki v tem času ne morejo opravljati svojega dela (K3=3).

5/1: stalna prisotnost vsaj dveh zaposlenih v IT se lahko doseže precej hitro (K1=4). Dobro rešuje problem nadomeščanja (K2=3). Strošek je v roku službe (K3=4).

5/2: uvajanje nadomestljivega kadra za izredne razmere zahteva predhodno pripravo in ga ni mogoče uvesti takoj (K1=3). Dokaj učinkovito lahko reši problem nadomeščanj (K2=4). Ne zahteva dodatnih stroškov, ker so vključeni notranji zaposleni (K3=4).

5/3: z nekaj predhodne priprave se bazo znanja da vzpostaviti sorazmerno hitro (K1=4). Dobro lahko prispeva k nadomeščanju kadra (K2=3). Strošek je v roku službe (K3=4).

5/4: specialna baza znanja v obliki diagramov poteka je teže uresničljiva (K1=2). Dobro lahko reši problem nadomeščanja tudi v IT oddelku (K2=3). Stroški so zajeti v roku službe (K3=4).

1.) Iskanje rešitev za predlog vrzeli "pametni telefoni" (2. org.)

Komentar udeležencev med iskanjem rešitev:
Tak telefon je prikladnejši od prenosnega računalnika, ker ga lahko nosimo v žepih, torbicah, tablično izvedbo pa v mapah ali manjšem poslovnem nahrbtniku. Verjetnost kraje ali možnost, da ga kje pozabimo, sta zato še toliko večja. Če pogledamo vsebino službenega telefona, so kontakti poslovnih partnerjev javni in dostopni na Ajpesu[12]. Problem lahko predstavlja edino elektronska pošta. Kar je zaupne pošte, je zaščitena s PGP-jem. Najti je treba pravo mejo med varnostjo in zaupanjem. Če ni nobenega zaupanja, je nesmiselno uporabljati službene telefone. Pohod nove tehnologe je neizogiben, čez nekaj let bo verjetno sleherni zaposleni imel pametni telefon in dostop še do česa drugega, kot so Facebook, Twitter, Google ipd.

Predlogi rešitev vrzeli:
- dostop do elektronske pošte na telefonu mora biti obvezno zaščiten z geslom ob upoštevanju osnov izbire "močnejšega gesla"[13], obvezno je tudi zaklepanje telefona v stanju pripravljenosti z geslom;
- interni pravilnik, ki določa zaklepanje delovnih postaj ko se začasno zapusti delovno mesto (malica, sestanki ipd.), se razširi tudi na uporabo pametnih telefonov.

Končni predlog rešitve skupine za vrzel:
- dostop do elektronske pošte na telefonu mora biti obvezno zaščiten z geslom ob upoštevanju osnov izbire "močnejšega gesla", obvezno je tudi zaklepanje telefona v stanju pripravljenosti z geslom.

2.) Iskanje rešitev za predlog vrzeli "pravilna konfiguracija varnostnih elementov omrežja" (2. org.)

Komentar udeležencev med iskanjem rešitev:
Ti elementi predstavljajo most med internim omrežjem organizacije in zunanjim, prostranim WAN omrežjem, kamor sodijo internetna povezava kot tudi najete linije do poslovnih partnerjev, podizvajalcev in strank. Še posebej dostop do interneta mora biti skrbno načrtovan. Nujno je redno spremljanje in nameščanje popravkov internega programja (firmware) kot tudi operacijskih sistemov teh elementov (stikal, usmerjevalnikov, požarnih zidov).

[12] Ajpes – agencija Republike Slovenije za javnopravne evidence in storitve.
[13] Geslo, ki je dolgo vsaj sedem znakov, med katerimi so tudi neabecedni znaki in številke.

Predlogi rešitev vrzeli:

- pri nastavitvah konfiguracije morata biti vedno prisotna dva iz IT oddelka, ki se medsebojno dopolnjujeta in kontrolirata;
- redno spremljanje razvoja programskih orodij, ki omogočajo kontrolo teh nastavitev za izključitev možnih napak;
- stalno izobraževanje pri partnerjih, ki tržijo to specialno opremo (CISCO, Huawei, itd.).

Končni predlog rešitve skupine za vrzel:

- redno spremljanje razvoja programskih orodij, ki omogočajo kontrolo teh nastavitev za izključitev možnih napak.

3.) Iskanje rešitev za predlog vrzeli "strukturni kapital" (2. org.)

Komentar udeležencev med iskanjem rešitev:
V delu razvoja je že doslej praksa, da se vse specifikacije in tudi ideje posameznikov pošiljajo na izbrani poštni seznam, kar pomeni, da se nasledniki reševanja že začetega problema tako ne ukvarjajo ponovno z vsem od začetka. Uporabljajo t. i. interno Wiki[14] bazo znanja (podobno kot Wikipedia), ki je definirana na ravni celotne organizacije. Trenutno kaže na to, da jo večinoma uporablja le razvoj. Organizirana je stopenjsko, tako da določene dele baze znanja lahko vidi le izbrani krog uporabnikov. V tej bazi so različna navodila za uporabo, ki jih lahko vidijo vsi v organizaciji, do specifikacij protokolov in različnih arhitektur, ki jih vidijo le izbrani posamezniki. Verjetnost, da bi se v nekem trenutku zamenjalo več ključnih kadrov, je majhna. Praksa je, da v primeru da kdo npr. obišče nek sejem v tujini, deli to izkušnjo z ostalimi v oddelku.

Predlogi rešitev vrzeli:

- interno Wiki bazo znanja naj se v skladu s sedanjo prakso razvojnega oddelka razširi še na ostale oddelke;
- proces dela z bazo znanja še bolj zastaviti v smeri, da bo skozi dokumentacijo prenos znanja iz razvoja potekal kar se da tekoče tudi do ostalih zainteresiranih oddelkov in skupin;
- s selektivnim dostopom do baze znanja še bolje pokriti zamenljivost ključnih kadrov (primeri bolniških izostankov, nepredvideni dogodki, odhodi ključnih oseb iz organizacije itd.). Zamenljivost teh oseb je sicer že doslej sorazmerno dobro organizirana in pokrita, lahko pa se jo še izboljša.

Končni predlog rešitve skupine za vrzel:

- proces dela z bazo znanja še bolj zastaviti v smeri, da bo skozi dokumentacijo prenos znanja iz razvoja potekal kar se da tekoče tudi do ostalih zainteresiranih oddelkov in skupin.

[14] Wiki – podjetniška Wiki-enciklopedija za dokumentiranje znanja, temelječega na izkušnjah.

4.) Iskanje rešitev za predlog vrzeli "kraja prenosnika, medijev USB" (2. org.)

Komentar udeležencev med iskanjem rešitev:
Pri prenosnih računalnikih so najbolj ranljivi zaposleni iz določenih delov razvoja. Gre lahko za krajo prenosnika, npr. iz avta, na službeni poti ipd., verjetnost, da kdo pride do podatkov, pa je majhna. Večina delovnega gradiva po ostalih oddelkih je na strežnikih. V razvoju se uporabljajo USB ključki, na katerih so TrueCrypt[15] particije. V preteklosti je enkrat že bila izpostavljena možnost, da se dostop do USB vrat (portov) zapre. Na ta način se ključkov enostavno ne bi dalo uporabljati. V kontekstu USB ključev je bil omenjen tudi sodobni mobilni telefon. Tega se prav tako lahko priključi na računalnik preko USB vhoda in igra vlogo zunanje diskovne enote.

Predlogi rešitev vrzeli:
- na prenosniku morajo imeti vsi vključeno opcijo zaklepanja diskovne enote in uporabljati možnost kriptiranja (kodiranja) podatkov na disku. Zahtevana dosledna uporaba gesel za kriptiranje na USB ključih;
- prepoved uporabe USB ključkov.

Končni predlog rešitve skupine za vrzel:
- na prenosniku morajo imeti vsi vključeno možnost zaklepanja diskovne enote in uporabljati kodiranje (kriptiranje) podatkov na disku. Zahtevana je tudi uporaba gesel in kriptiranja na USB ključkih.

5.) Iskanje rešitev za predlog vrzeli "pridobitev uporabniškega imena in gesla" (2. org.)

Komentar udeležencev med iskanjem rešitev:
Pri tem je glavni problem človeška naivnost. Vzemimo za primer, da nekdo od zaposlenih pokliče drugega zaposlenega, naj mu posodi geslo za dostop do nečesa, kar ravnokar potrebuje pri svojem delu. V 90 % se to lahko tudi zgodi. Lahko je postavljen izvrsten varnostni sistem, toda neozaveščeni zaposleni bodo še vedno "največja luknja" varnosti. Prav zato je treba zaposlene o tem stalno ozaveščati - za te aktivnosti so še posebej poklicani tisti, ki so zadolženi za informacijsko varnost v organizaciji. To lahko izpeljejo tako, da se s posameznimi skupinami zaposlenih občasno zberejo in s kakšno predstavitvijo razpravljajo o tej problematiki. Pomembno je graditi na zaupanju, ki pa ga lahko pridobimo le z zdravo klimo in ustrezno kulturo v organizaciji.

Predlogi rešitev vrzeli:
- učinkovita je rešitev, da se vse zaposlene jasno seznani s tem, da se gesla v nobenem primeru ne sme posoditi ali povedati;
- na tem je treba stalno in periodično delovati in preverjati stanje;

[15] Programska oprema za kriptiranje podatkov na različnih medijih.

- nenehno je treba graditi na bistvenem elementu, tj. na zaupanju med zaposlenimi v organizaciji.

Končni predlog rešitve skupine za vrzel:
- učinkovita je rešitev, da se vse zaposlene jasno seznani s tem, da se gesla v nobenem primeru ne sme posoditi ali povedati.

Preglednica 19: Povzetek predlogov rešitev za izbrane vrzeli (2. org.)

Številka predloga →	1	2	3	4	5
Številka rešitve ↓	Pametni telefoni	Pravilna konfig. varn. elem. omrežja	Strukturni kapital	Kraja prenosnika in medijev USB	Pridobitev uporabniškega imena in gesla
1	Dostop do * elektronske pošte na telefonu mora biti obvezno zaščiten z geslom	Pri nastavitvah konfiguracije morata biti vedno prisotna dva iz IT oddelka	Interno Wiki bazo znanja se razširi na ostale oddelke	Prenosniki morajo imeti vključeno opcijo zaklepanja disk. enote in uporabo kriptiranja podatkov	Zaposlene jasno seznaniti, da se gesla v nobenem primeru ne sme posoditi
2	Interni pravilnik, ki določa zaklepanje delovnih postaj, se razširi tudi na uporabo pametnih telefonov	Redno spremljanje razvoja programskih orodij	Delo z Wiki bazo znanja zastaviti v smeri prenosa znanja iz razvoja do ostalih oddelkov	Prepoved uporabe USB ključkov	Stalno periodično delovanje na tem področju in preverjanje stanja
3		Stalno izobraževanje pri partnerjih, ki tržijo to specialno opremo	Selektivni dostop do baze znanja in zamenljivost ključnih kadrov		Graditi na zaupanju med zaposlenimi v organizaciji

* Senčeno polje označuje končni predlog rešitve za posamezno vrzel na srečanju skupine.

Za ocenjevanje predlaganih rešitev uporabimo podobno kot pri raziskavi v prvi organizaciji metodo glavnih dejavnikov uspeha (KSF). Pri tem upoštevamo izbrane kriterije in uteži iz preglednice 17 na strani 63.

Preglednica 20: Ocenjevanje rešitev varnostnih vrzeli z metodo KSF (2. org.)

Številka predloga/rešitve	K1 Izvedljivost	U1	K2 Učinkovitost	U2	K3 Cena	U3	Vrednost rešitve (VR)
	1-5*	1-3	1-5*	1-3	1-5*	1-3	K1×U1+K2×U2+K3×U3
1 / 1	5	3	4	2	5	1	28
1 / 2	4	3	3	2	4	1	22
2 / 1	5	3	5	2	5	1	30
2 / 2	5	3	5	2	5	1	30
2 / 3	5	3	4	2	3	1	26
3 / 1	4	3	3	2	4	1	22
3 / 2	5	3	4	2	4	1	27
3 / 3	4	3	3	2	4	1	22
4 / 1	5	3	5	2	5	1	30
4 / 2	5	3	5	2	5	1	30
5 / 1	5	3	3	2	5	1	26
5 / 2	5	3	3	2	4	1	25
5 / 3	4	3	4	2	5	1	25

* Kriteriji K1, K2 in K3 se ocenjujejo z vrednostno oceno med 1 in 5, kot je prikazano spodaj.

K1 – izvedljivost: (5) izvedljivo takoj oz. zelo hitro, (4) izvedljivo z nekaj predhodne priprave, (3) izvedljivo na daljši rok, (2) izvedljivost je zadovoljiva, (1) ni izvedljivo.

K2 – učinkovitost: (5) zelo učinkovito, (4) dokaj učinkovito, (3) učinkovitost je dobra, (2) zadovoljiva učinkovitost, (1) neučinkovito.

K3 – cena: (5) stroškov ni, (4) strošek gre v rok službe, (3) cenovno ugodno, (2) sorazmerno visoka cena, (1) zelo visoka cena, drago.

Argumenti ocenjevanja kriterijev v preglednici 20 (2. org.)

1/1: ukrep obvezne zaščite dostopa do elektronske pošte na telefonu je hitro izvedljiv (K1=5). Dokaj učinkovito vpliva na informacijsko varnost v primeru kraje (K2=4). Stroškov z uvedbo praktično ni (K3=5).

1/2: dodatek k internemu pravilniku je mogoč v sorazmerno kratkem času (K1=4). Dobro vpliva na spoštovanje informacijske varnosti (K2=3). Zadevo lahko uredi pravna služba organizacije v roku službe (K3=4).

2/1: interno pravilo IT oddelka glede nastavitev varnostnih elementov je mogoče vpeljati takoj (K1=5). Problem tovrstnih napak se učinkovito reši (K2=5), stroška z uvedbo ni (K3=5).

2/2: interno pravilo IT oddelka za redno spremljanje razvoja programskih orodij je hitro uresničljivo (K1=5), učinkovito rešuje morebitne nove varnostne grožnje (K2=5), izvaja se v roku službe (K3=5).

2/3: interno pravilo IT oddelka glede izobraževanja pri partnerjih, ki tržijo specialno opremo, je hitro uresničljivo (K1=5). Učinkovito vpliva na večjo zanesljivost pri uporabi opreme (K2=4). Glede na partnerstvo je organizacija deležna popusta (K3=3).

3/1: hitra možnost vpeljave baze znanja v ostale oddelke (K1=4). Dobro vpliva na storilnost in ohranjanje znanja v organizaciji (K2=3). Aktivnost ni povezana s posebnimi stroški, izvaja se v roku službe (K3=4).

3/2: prenos znanja iz razvoja do ostalih oddelkov preko interne baze je hitro mogoč (K1=5). Dokaj učinkovito lahko vpliva na pretok znanja in storilnost ostalih oddelkov (K2=4). Aktivnost je povezana z administracijo interne Wiki baze v roku službe (K3=4).

3/3: ukrep administratorja interne baze znanja je mogoč dokaj hitro (K1=4). Dobro lahko reši problem nadomeščanj (K2=3). Vključeno je delo zaposlenega v roku službe (K3=4).

4/1: gre za ukrep zaklepanja disk. enote in uporabo kriptiranja podatkov, ki ga je mogoče sprejeti takoj (K1=5). Učinkovito rešuje problem kraje pametnega telefona (K2=5). S tem ni dodatnih stroškov (K3=5).

4/2: ukrep morebitne prepovedi uporabe USB ključkov je mogoč takoj (K1=5). Učinkovito rešuje problem kraje podatkov (K2=5). Ne zahteva posebnih dodatnih stroškov (K3=5).

5/1: ukrep glede seznanitve izposoje gesla je mogoč takoj (K1=5). Prispeva k informacijski varnosti, traja pa lahko nekaj časa, da ga uporabniki dosledno spoštujejo (K2=3). Ne zahteva posebnih dodatnih stroškov (K3=5).

5/2: za periodično delovanje v tej smeri je mogoča vpeljava takoj (K1=5). Dobro vpliva na informacijsko varnost (K2=3). Zadolžitve so v roku službe, zato ni posebnih dodatnih stroškov (K3=4).

5/3: dogovor o tem je mogoče sprejeti sorazmerno hitro (K1=4). Učinkovito rešuje problem informacijske varnosti (K2=4). Ne zahteva dodatnih stroškov, le voljo in željo zaposlenih (K3=5).

Faza 3A se z ocenjevanjem rešitev in izračunom rezultatov zaključi.

Faza 3B – študija izvedljivosti in izbor rešitev varnostnih vrzeli IS

V preglednici 21 za prvo in preglednici 22 za drugo organizacijo so predlogi rešitev varnostnih vrzeli IS razvrščeni v skladu s KSF oceno avtorja magistrske naloge. V skrajnem desnem stolpcu je predstavljena ocena kriterija izvedljivosti posamezne rešitve. Pri ocenjevanju smo temu kriteriju dali najvišjo utež. Dobiti želimo predvsem izvedljive in učinkovite rešitve za posamezno vrzel IS.

Preglednica 21: Rezultati ocenjevanja rešitev varnostnih vrzeli (1. org.)

	Številka predloga/rešitve	Predlog rešitve za vrzel	Vrednost rešitve (VR)	K1 Izvedlj.
	1 / 2	Nakup dodatnih uporabniških licenc ERP sistema	26	5
*	3 / 1	Nakup novega VPN sistema	26	5
	2 / 1	Hitra optična povezava do rezervne lokacije arhivskih podatkov	25	5
	4 / 1	Sistemska nastavitev kontrole kakovosti in periodične menjave gesel	24	5
	2 / 2	Arhiviranje podatkov pri zunanjem ponudniku	23	4
	1 / 1	Graditi na zaupanju in ozaveščenosti obstoječih in novih uporabnikov	22	3
	3 / 2	Omejitev VPN dostopov	22	3
	5 / 1	Vedno 50 % zasedenost IT oddelka, stalna prisotnost vsaj dveh zaposlenih	22	4
	5 / 3	Vzpostavitev baze znanja prog. rešitve Helpdesk	22	4
	5 / 2	Uvajanje nadomestljivega kadra za izredne razmere	21	3
	4 / 2	Periodično naključno izvajanje nadzora gesel in disciplinsko ukrepanje	20	3
	5 / 4	Specialna baza znanja v obliki diagramov poteka	16	2

* Senčena polja označujejo končni predlog rešitve skupine za posamezno vrzel.

Senčena polja označujejo končne izbrane rešitve skupine z 2. srečanja. Pri izbiri damo prednost tistim rešitvam, ki so po KSF ocenjevanju najbolje uvrščene in hkrati sovpadajo s končnimi izbranimi rešitvami skupine. Druga, tretja in četrta rešitev sovpadajo s KSF oceno. Vse so hitro izvedljive, kar kaže najvišja ocena kriterija izvedljivosti. Pri odločitvi, kateri rešitvi bi kot tretji dali prednost, ocenjeni s strani avtorja ali končni predlagani rešitvi skupine, si pomagamo z oceno iz tabele tveganja. Napravili smo jo pri analizi vrzeli v preglednici 13. Za vrzel dostopa do ERP sistema smo dobili najvišjo možno oceno tveganja, to je 7, vrzel

uganljivih gesel pa je prejela oceno 5. Ker želimo tveganje zmanjšati, se v tem primeru odločimo za rešitev nakupa dodatnih uporabniških licenc ERP sistema, za katero smo tudi po KSF oceni dobili najvišji seštevek. Vrednostna ocena te vrzeli je prikazana na sliki 8.

Preglednica 22: Rezultati ocenjevanja rešitev varnostnih vrzeli (2. org.)

	Številka predloga/rešitve	Predlog rešitve za vrzel	Vrednost rešitve (VR)	K1 Izvedlj.
	2 / 1	Pri nastavitvah konfiguracije (varnostni elementi omrežja) morata biti vedno prisotna dva iz IT odd.	30	5
*	2 / 2	Redno spremljanje razvoja programskih orodij (varnostni elementi omrežja)	30	5
	4 / 1	Prenosniki morajo imeti vključeno opcijo zaklepanja diskovne enote in uporabo kriptiranja podatkov	30	5
	4 / 2	Prepoved uporabe USB ključkov	30	5
	1 / 1	Dostop do elektronske pošte na pametnem telefonu mora biti obvezno zaščiten z geslom	28	5
	3 / 2	Delo z Wiki bazo znanja usmeriti v prenos znanja iz razvoja do ostalih oddelkov	27	5
	2 / 3	Stalno izobr. pri partnerjih, ki tržijo special. opremo (varnostni elementi omrežja)	26	5
	5 / 1	Zaposlene jasno seznaniti, da se gesla v nobenem primeru ne sme posoditi	26	5
	5 / 2	Stalno periodično delovanje na tem področju in preverjanje stanja	25	5
	5 / 3	Graditi na zaupanju med zaposlenimi v organizaciji	25	4
	1 / 2	Interni pravilnik, ki določa zaklepanje delovnih postaj, se razširi tudi na uporabo pametnih telefonov	22	4
	3 / 1	Interno Wiki bazo znanja se razširi na ostale oddelke	22	4
	3 / 3	Selektivni dostop do baze znanja in zamenljivost ključnih kadrov	22	4

* Senčena polja označujejo končni predlog rešitve skupine za posamezno vrzel.

Prvi štirje predlogi rešitev so prejeli enako KSF oceno in faktor izvedljivosti. Ob razvrščanju teh rešitev pri vsaki ponovno pogledamo prejeto oceno tveganja povezane vrzeli. Dobili smo jo pri analizi vrzeli v preglednici 14.

Prvih sedem predlogov rešitev v preglednici 22 je povezanih s štirimi varnostnimi vrzelmi, ki so v tabeli tveganja prejele naslednje ocene:

- pravilna konfiguracija varnostnih elementov omrežja (ocena tveganja=6);
- kraja prenosnika in medijev USB (ocena tveganja=4);
- pametni telefoni (ocena tveganja=6);
- strukturni kapital (ocena tveganja=5).

Prvi dve rešitvi preglednice sta povezani z varnostno vrzeljo Varnostnih elementov omrežja, naslednji dve pa z vrzeljo Kraje prenosnika in medijev USB. Za vrzel Varnostnih elementov omrežja je bilo s tabelo ugotovljeno večje tveganje. Prednost med obema rešitvama te vrzeli damo tisti, ki jo je izbrala tudi skupina. Na tej osnovi pridemo do prve izbrane rešitve:

- redno spremljanje razvoja programskih orodij varnostnih elementov omrežja

V tabeli ocene tveganja sledita vrzeli Pametnih telefonov in Strukturnega kapitala. V preglednici 22 poiščemo najbolje uvrščene rešitve, ki so povezane z njima. Rešitev dostopa do elektronske pošte na pametnem telefonu ima nekoliko nižjo KSF oceno. Prednost ima večje tveganje z njo povezane vrzeli, zato kot drugo rešitev izberemo:

- dostop do elektronske pošte na pametnem telefonu mora biti obvezno zaščiten z geslom

Podobno se odločimo tudi za naslednjo rešitev. Po ocenjenem tveganju v preglednici 14 je vrzel strukturnega kapitala na tretjem mestu. Kljub slabši KSF oceni, ki rešitev uvršča po izvedljivosti, učinkovitosti in ceni, se odločimo za rešitev, katere vrzel predstavlja večje varnostno tveganje:

- delo z Wiki bazo znanja usmeriti v prenos znanja iz razvoja do ostalih oddelkov

Glede na izvedeno študijo bomo vodstvu organizacij predlagali rešitve za izboljšanje njihove informacijske varnosti, ki jih povzemamo v preglednici 23.

Preglednica 23: Končne rešitve ranljivosti IS, predlagane za izvedbo

Prva organizacija	Druga organizacija
Nakup dodatnih uporabniških licenc ERP sistema	Redno spremljanje razvoja programskih orodij varnostnih elementov omrežja
Nakup novega VPN sistema	Dostop do elektronske pošte na pametnem telefonu mora biti obvezno zaščiten z geslom
Hitra optična povezava do rezervne lokacije arhivskih podatkov	Delo z Wiki bazo znanja usmeriti v prenos znanja iz razvoja do ostalih oddelkov

Faza 3B je s tem zaključena.

Faza 3C – posamični polstrukturirani intervju z vodji IT in kritična analiza

Zadnje srečanje v organizacijah je predstavljal polstrukturirani intervju z vodjo službe za informatiko v prvi in vodjo sistemske administracije ter člani ožjega vodstva v drugi organizaciji. Vodilo srečanja je predstavljalo šest vprašanj iz priloge 7. Polstrukturirani intervju za prvo organizacijo predstavljamo v prilogi 13, za drugo pa v prilogi 14.

Kritična analiza za realizacijo predlaganih rešitev (1. in 2. org.)

Rezultati uporabljene inovativne metode v praksi so prikazani v levem stolpcu preglednice 23 za prvo in v desnem stolpcu za drugo organizacijo. Izbrani inovativni posamezniki so na možne vrzeli IS opozorili na prvem srečanju skupine. Do začetka drugega srečanja so jih ocenjevali kompetentni vodje iz posameznih oddelkov (nivojev organizacije). Njihovo končno razvrstitev je z analizo vrzeli izvedel avtor magistrske naloge. Usklajene predloge rešitev za razvrščene vrzeli so udeleženci določili na drugem srečanju skupine. V preglednici 21 za prvo in preglednici 22 za drugo organizacijo so vsi predlogi razvrščeni še glede na dobljeno KSF oceno. Ocenjevanje je izvedel avtor magistrske naloge. Analiza treh končnih rešitev, ki bodo vodstvu organizacij predlagane za izvedbo, je predstavljena v nadaljevanju.

Srednje velike organizacije danes brez ERP sistema težko sledijo konkurenci. Ta vir ima zanje veliko vrednost. Uporabniške licence so drage, razen če ne gre za lastne rešitve. Grožnja informacijski varnosti v primeru odpovedi je velika. Zato takega sistema ne sme izpustiti nobena odgovorna varnostna politika organizacije. V organizacijah se zahteva več kot 98 % razpoložljivost bistvenih elementov IS. Na letni ravni pomeni ta odstotek dober teden dni nedelovanja sistema, v kar so všteti vsi napovedani in nenapovedani izpadi. Dovoljena izguba podatkov je ponavadi največ en delovni dan. Organizacije lahko prispevajo k varnosti svojih podatkov z načrtovanjem zadostnega števila uporabniških licenc, da ne bi zaradi ohlapno dodeljenih pravic na bazi podatkov (rol) v primeru da z eno licenco delata celo dva, prihajalo do napak s strani še ne dovolj usposobljenih uporabnikov. Investicija v potrebne dodatne licence se kmalu povrne, ker tudi napake, ki se lahko zgodijo v prej opisanem primeru, niso zastonj. Če do njih pride, je delo dvojno, povzročijo pa lahko celo izgubo ugleda organizacije pri kupcih, dobaviteljih in ostalih strankah.

Zaradi hitrosti dostopa v primeru težav ali enostavnejših nadgradnjah programske opreme organizacije omogočajo zunanjim vzdrževalnim službam pa tudi svojim uporabnikom dostop do notranjega komunikacijskega omrežja preko VPN povezav. K varnosti dostopa prispeva uporaba geselnikov in podobnih naprav za generiranje gesla pri prijavi. Na ta način se v veliki meri prepreči vdore v omrežje s pomočjo avtomatskih generatorjev gesel. K varnosti doda svoje tudi vrsta sistema, ki dostop omogoča. Zagotavljati mora selektivni dostop do

strežnikov organizacije in natančno spremljanje, kdo se je prijavil, kdaj, koliko časa je bil aktiven na sistemu in katere aktivnosti je izvajal.
Varnost podatkov je odvisna tudi od tega, kako se izvaja njihovo zaščitno kopiranje. Dobra praksa je, da se kopije podatkov hranijo na dveh fizično oddaljenih lokacijah. Pri tem mislimo na hranjenje arhivskih podatkov in dnevnega zaščitnega kopiranja. Med lokacijami je običajno vzpostavljena hitra optična povezava, ki omogoča velike prenosne hitrosti. Organizacije imajo danes možnost, da arhiviranje v celoti prepustijo kvalificiranim zunanjim ponudnikom. Teh je v zadnjem času vedno več, zato so cene te storitve dostopnejše. V tem primeru organizaciji ni treba skrbeti za potrebno opremo in njeno posodabljanje, zagotavlja jo zunanji ponudnik. Ker je izpostavljen trgu, mora s posodobitvami aparaturne in programske opreme neprestano skrbeti, da ohranja konkurenčno prednost. To za organizacije pomeni, da so njihovi podatki varni in na razpolago, ko jih potrebujejo.

V prilogi 8 smo na primeru ponazorili, katera znanja naj ima sistemski administrator, da lahko izvaja nastavitve na varnostnih elementih omrežja. Predlaga se tudi, da so to zaposleni z opravljenimi izpiti v pooblaščenih centrih izdelovalca tovrstne specialne opreme. Da zaposleni doseže ta nivo znanja, organizacija vanj veliko investira, zato zanjo predstavlja veliko vrednost in nastane tudi precejšnja škoda, če npr. zaposleni odpove delovno razmerje. Njegova prisotnost v organizaciji je neposredno povezana z informacijsko varnostjo. Redno spremljanje novosti na specialni opremi, kot so usmerjevalniki in požarni zidovi, mora biti dnevno, kot je zasledovanje pojava novih virusov. Sem spada tudi sodelovanje na spletnih forumih, kjer si informacije, opozorila in postopke izmenjujejo specialisti IT. Varnostna politika organizacije mora predvideti vsaj dva usposobljena zaposlena iz IT oddelka v ta namen. S tem se pokrije nadomeščanje za primere odsotnosti oz. odpoved delovnega razmerja. V zadnjem primeru je potrebno še posebej paziti na to, da se odhajajočemu zaposlenemu odvzamejo vsa pooblastila, ki jih je imel za delo na IS.

S pravilnimi nastavitvami varnostnih elementov omrežja (usmerjevalnikov, požarnih zidov in komunikacijskih stikal) se v organizacijah lahko prepreči marsikatero grožnjo vdora v interni komunikacijski sistem. Dandanes je ta nevarnost vse večja, še posebej z uporabo pametnih telefonov. Priporočljivo je, da se pri pomembnih nastavitvah med seboj kontrolirata dva specialista s področja IT. Vsako pomembno akcijo je treba najprej dobro pretehtati, uskladiti in šele nato izvesti. Po končanih nastavitvah je pametno dostop omejiti izključno na ožje vodstvo IT oddelka, ki mora vsako spremembo jasno dokumentirati. Proizvajalci profesionalne opreme svojo programsko opremo nenehno prilagajajo v skladu z izzivi na trgu komunikacijskih naprav, razvojem novih vrst protokolov itd. Redno izdajajo tudi popravke za svoje produkte, v primeru da se naknadno izkažejo napake v njej ali varnostne "luknje". Če povzamemo: K informacijski varnosti lahko prispevajo zaposleni IT oddelkov v veliki meri s tem, da redno posodabljajo komunikacijsko varnostno opremo in spremljajo razvoj novih programskih orodij.

Imetnikov pametnih telefonov je v organizacijah vse več. Uporabnikom omogočajo, da na službeni poti doma ali v tujini spremljajo delo na projektih, prebirajo službeno elektronsko

pošto, so dostopni po telefonu in preko SMS sporočil, uporabljajo satelitske navigacijske programe itd. Prav zaradi odprtosti in širine uporabe lahko pride do zlorabe podatkov ali celo vdora v interni komunikacijski sistem. Še posebej so nevarne vključene možnosti brezžičnega dostopa do omrežja, na katere smo opozorili v teoretičnem delu naloge. Varnostna politika v organizacijah mora zato upoštevati dosledno zaklepanje takšnih telefonov z gesli, ki se težko uganejo. Podobno velja tudi za programske rešitve, ki se na telefonih uporabljajo. Mednje sodijo odjemalci elektronske pošte. Uporabniki sami lahko največ prispevajo k informacijski varnosti s tem, da pazijo in teh naprav ne puščajo nikjer brez nadzora, kar še posebej velja za javna mesta.

Za visokotehnološke organizacije, kjer večina zaposlenih dela na projektih z visoko dodano vrednostjo, je izrednega pomena, da se njihova znanja in kompetence v kar največji možni meri strukturirajo. Če organizacija v znanje zaposlenih vlaga svoja sredstva, lahko na drugi strani zahteva od njih, da pridobljena znanja kar najbolje dokumentirajo v vzpostavljeni interni bazi znanja. Danes je na trgu dovolj tovrstne programske opreme, tako da se za vsako organizacijo lahko najde najprimernejša. Taka baza znanja mora imeti skrbnika, vodje posameznih oddelkov pa je treba zadolžiti, da skrbijo za recenzijo vsebine svojih podrejenih. Čim več znanja se iz glav zaposlenih prenese v strukturirano obliko, tem manjša je grožnja po izgubi, če kdo od zaposlenih npr. da odpoved ali se zgodi kaj nepredvidenega. Tako pridobljeno znanje je last organizacije, zahteva pa selektiven dostop, še posebej, če gre za specialna znanja s področja informacijske varnosti. Bistveno je, da se znanje čim bolj širi med posameznimi oddelki. Na novo zaposleni v organizaciji se ob tako vzpostavljeni bazi znanja lahko hitreje vpeljejo v novo okolje in delo, mentorjem pa ni potrebno ponavljati vedno istih stvari, temveč jih le usmerjajo skozi gradivo v bazi, ki ga nato zaposleni samostojno študirajo.

5 VREDNOTENJE REZULTATOV RAZISKAVE

Raziskavo smo izvedli v dveh srednje velikih industrijskih organizacijah v privatni lasti. S svojimi izdelki in storitvami ustvarjata na trgu visoko dodano vrednost. Da bi preverili tudi drugo raziskovalno vprašanje naloge, smo k raziskavi povabili organizacijo, ki na informacijsko varnostnem področju odstopa od povprečja v Sloveniji. Ima mednarodni certifikat ISO 27001:2005 s področja varovanja informacij o poslovnih partnerjih in internih informacij.

5.1 Ocena rezultatov naloge s strani izboljšanja informacijske varnosti v organizacijah

Z vpeljavo teoretičnega modela povečanja varnosti IS v obeh organizacijah, izbiro poiskanih predlogov ranljivosti IS (ocenjevanje s kriterijem pomembnosti) in nadaljnjim preverjanjem s kvalitativnimi metodami (SWOT, tabela ocene tveganja, Schneierjevo drevo napada in KSF) smo dobili predloge izbranih rešitev, katerih vpeljava bo zagotovo odpravila odkrite nevarnosti IS in pozitivno prispevala k informacijski varnosti.

Dobljeni rezultati v obeh organizacijah kažejo razen pri dokumentacijskih podatkih, uporabniški programski opremi in prenosnih računalnikih na različna področja IS. Skladno z izbiro virov kategorizacije dobimo na koncu rezultate za odkrite ranljivosti. Kategorizacijo je zato treba napraviti skrbno, s poznavanjem IS in razmer v organizaciji. S tem dosežemo, da na prvem srečanju skupine (možganska nevihta) pomembnih ranljivosti ne izpustimo. Rešitve druge organizacije kažejo, da gre za zrelo organizacijo, na sliki 2 jasno umeščeno v strateškem delu. V primerjavi s prvo organizacijo zadevajo njihove rešitve opazno višjo raven virov (pametni telefoni, usmerjevalniki komunikacijskega prometa, požarni zidovi, strukturni kapital itd.). To verjetno ni naključno. Organizacija že dobro leto posluje v skladu s pridobljenim mednarodnim certifikatom ISO 27001:2005 s področja varovanja informacij o poslovnih partnerjih in internih informacij.

5.2 Finančni vidik dobljenih rešitev

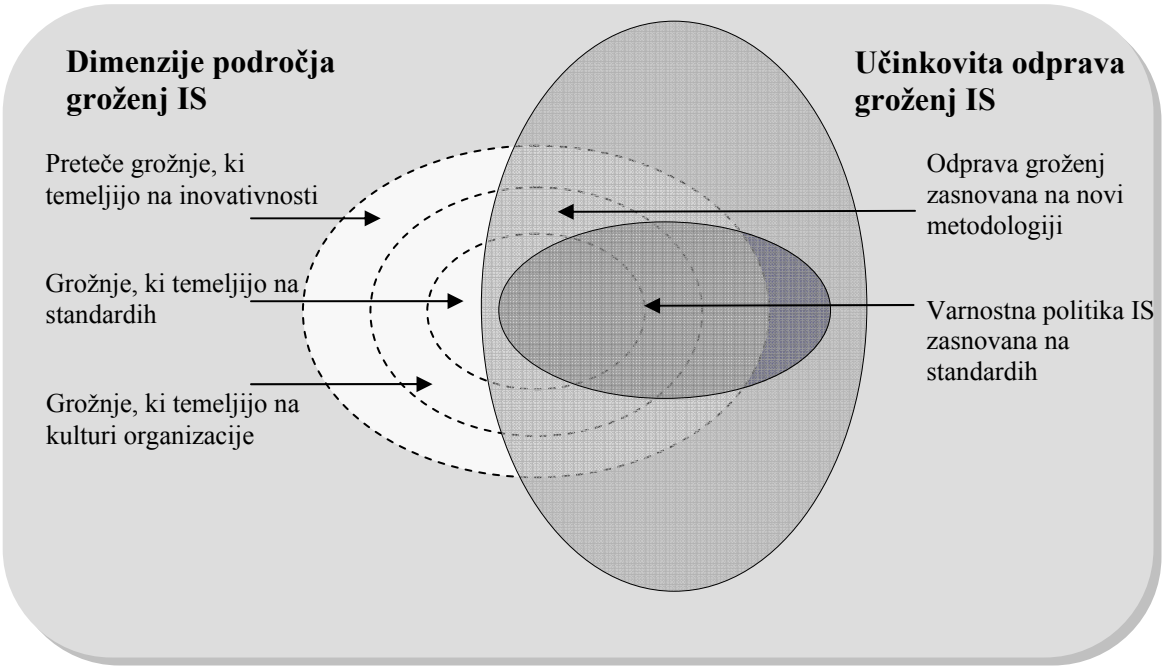
Na polstrukturiranem intervjuju smo sogovornikom v obeh organizacijah zastavili vprašanje, če lahko v grobem ocenijo oportunitetni strošek v EUR za ugotovljeno največjo nevarnost IS s strani njihove skupine. V prvi organizaciji je šlo za dostop uporabnikov do ERP sistema. Vodja službe za informatiko je odgovoril, da bi bilo treba napraviti podrobnejšo analizo tega predloga z upoštevanjem vseh okoliščin morebitnega incidenta na ERP sistemu. Spomnil je, da je organizacija OEM partner svetovno znanih koncernov v Evropi, s prepoznavnimi blagovnimi znamkami. Organizacija namreč v celoti izpelje razvoj in izdelavo posameznih sklopov za te stranke. ERP sistem podpira izdelavo teh sklopov vsaj s tremi moduli. To so nabava, proizvodnja in finance. Vzemimo primer, da gre za izdelavo komaj dobro razvitega posebnega sklopa, za katerega se še pripravlja patentno zaščito. Vsi detajli takega sklopa se obdelujejo v vseh prej omenjenih modulih ERP sistema. Uhajanje strateških informacij, kot je zatrdil naš sogovornik, lahko predstavlja za organizacijo škodo velikosti 10.000 do nekaj 100.000 EUR. Običajno gre v teh primerih za velikoserijsko proizvodnjo. Pri tem je treba

upoštevati še padec ugleda organizacije, morebitno ustavitev bodočih naročil itd. Prej ocenjeni znesek se tako še pomnoži. Z neprevidnim ravnanjem uporabnikov s podatki ERP sistema, morebitnimi napakami in neupoštevanjem interne varnostne politike glede varovanja internih ali zaupnih informacij lahko pridemo do škode velikih razsežnosti. Točno oceno v evrih pa je za tak primer težko dati. Vidimo pa, da je doprinos vpeljave rešitve za to ranljivost s finančnega vidika lahko zelo velik in se prav gotovo splača vložiti trud vanjo. Direktor iz druge organizacije, kjer je bil med najbolje ocenjenimi rešitvami za varnostne vrzeli IS pametni telefon, nam je ob tem vprašanju dejal: "Okolje je dinamično in razmerja posameznih kategorij, ki so v igri določenega incidenta ali morebitne grožnje, se neprestano spreminjajo. Če se nekaj ne zgodi, se niti ne zavedamo, kaj vse bi to utegnilo potegniti za sabo. Tudi če se nekaj zgodi, se v prvem hipu ne ve, kakšna sta strošek in celotna škoda."

Podobne ocene bi lahko dobili tudi za primer neurejenega arhiva podatkov v prvi ali za morebitno napako pri konfiguraciji katerega od varnostnih elementov omrežja v drugi organizaciji. Strinjamo se lahko z besedami direktorja iz druge organizacije, da se velikokrat niti ne zavedamo vseh posledic, dokler se kaj res ne zgodi. Zato se je pri analizi ocene tveganja treba zelo dobro poglobiti v posamezni incident in skušati zanj predvideti kar največ možnih posledic, da nas te kasneje, če do incidenta pride, ne presenetijo.

5.3 Učinkovitost novega koncepta pri obvladovanju groženj

Predloga, pametni telefoni in strukturni kapital iz druge organizacije potrjujeta dogajanje na sliki 11.



Slika 11: Področja kjer z inovativno metodo lahko pričakujemo boljše rezultate

Vir: Likar in Trček 2012.

Slika prikazuje vrste groženj pri katerih z novim konceptom lahko pričakujemo boljše rezultate v primerjavi s standardnim pristopom, ki temelji na standardih in sprejeti varnostni politiki organizacije. Leve tri elipse kažejo ravni groženj IS. Notranja ponazarja grožnje temelječe na standardih. V srednji so zajete nevarnosti, povezane s kulturo organizacije. Zunanja elipsa pa opozarja na nove preteče nevarnosti. Presečišče teh elips, ponazorjeno na desni, predstavlja učinkovitost obeh pristopov skupaj. Če uporabimo prikazano metodo, lahko pričakujemo boljše rezultate (Likar in Trček 2012). Predlog "strukturni kapital" ustreza presečnemu delu, temelječem na kulturi organizacije, medtem ko "pametni telefoni" sodijo izrazito v področje prihajajočih nevarnosti. Prav na teh dveh segmentih z novo metodologijo lahko pričakujemo boljše rezultate (širše pokritje prikazanega področja pretečih groženj IS).

Da se organizacija odloči zgraditi bazo znanja, temelječo na izkušnjah, znanju in dobrih praksah zaposlenih, mora biti zrela in doseči nivo kulture, ki temelji na zaupanju in dobrih odnosih med zaposlenimi. Zaposleni morajo imeti občutek, da so potrebni in za svoje delo ustrezno nagrajeni, sicer svojega znanja ne bodo dali na razpolago ostalim. Enako velja, če so razlike v plačah med njimi prevelike, in to izvejo naključno, ker so sicer zaupne narave. V organizaciji brez razvite tovrstne kulture se zaposleni čutijo ogrožene, da bodo izgubili delo. Med njimi prevladujejo nezdravo rivalstvo, egoizem in skrivanje znanja. To se gotovo pozna

tudi na splošni klimi v organizaciji, če vodstvo tega ne zazna ali ni sposobno ukrepati ter urediti zadev v pozitivni smeri. Še boljše rezultate lahko doseže organizacija, če z ustrezno nagrajevalno politiko zaposlene dodatno stimulira tako, da tistega, ki v bazo znanja prispeva več in bolje oz. se kasneje celo izkaže, da je njegov oz. njen prispevek posredno pripeljal do novega proizvoda, dodatno nagradi. O kvaliteti prispevkov posameznikov naj bi presojali zaposleni s svojimi vodji na delovnih sestankih sami in z vnaprej izdelano vrednostno matriko. Rezultate in argumente pa bi potem njihov vodja predložil vodstvu organizacije. Tak način prepreči favoriziranje določenih posameznikov in pavšalnost, če bi o tem odločal nekdo drug.

5.4 Prispevek celotne metodologije k inovativnemu zagotavljanju varnosti

Pri oceni prispevka celotne metodologije na inovativno zagotavljanje varnosti IS lahko na kratko povzamemo besede sogovornikov iz obeh organizacij. V prvi je vodja službe za informatiko nov pristop reševanja problematike informacijske varnosti označil kot dobrodošel, ker so vanj vključeni tudi ostali zaposleni. Že s tem, ko aktivno sodelujejo, se dvigne njihova ozaveščenost o obravnavanih problemih. Bistveno je, da s svojo izkušnjo vplivajo tudi na ostale zaposlene. Proaktivno delovanje v tveganih situacijah in opozarjanje na probleme tako postane praksa.

Tudi sogovorniki iz druge organizacije so koncept označili kot še en pristop, ki dodatno vključuje zaposlene in omogoča, da se z drugega zornega kota pogleda, kje potencialne ranljivosti sistema še obstajajo. Konceptu pripisujejo prednost prav v razpršenosti in vključitvi zaposlenih iz celotne organizacije. Zaposleni, ki so sodelovali na prvem in drugem srečanju ter pri ocenjevanju predlogov, so pridobili dodatne izkušnje, ki jih bodo lahko širili na ostale zaposlene.

5.5 Vrednotenje raziskovalnih vprašanj

Za vsako raziskovalno vprašanje, ki smo ga zastavili v raziskavi, ločeno podajamo njegovo ovrednotenje.

Raziskovalno vprašanje 1: Ali predstavljena metodologija omogoča v izbranih organizacijah poiskati varnostne vrzeli IS in rešitve zanje, ki lahko prispevajo k izboljšanju varnosti obstoječega IS in pretoka informacij?

Z vpeljavo dobljenih rešitev v preglednici 23, lahko vsaka od obeh, obravnavanih organizacij na informacijsko varnostnem področju le pridobi. Razgovor z vodji IT in ostalimi vodilnimi v organizaciji je pokazal, da so se nekaterih odkritih ranljivosti sicer zavedali že doslej, na ostale pa so opozorili udeleženci organiziranih sej, torej zaposleni iz različnih oddelkov in ravni organizacije. S predstavljeno metodo so dobili možnost, da opozorijo na probleme in ranljivosti IS, ki jih vidijo s svojega delovnega mesta in jih tudi ovrednotijo (ocenijo) v okviru

svojih kompetenc. Dobljene rešitve bodo pozitivno prispevale tudi pri dopolnitvah obstoječih varnostnih politik in ocenah tveganja. To potrjuje naše prvo raziskovalno vprašanje.

Raziskovalno vprašanje 2: Ali s predstavljeno metodologijo lahko dosežemo dodano vrednost (pozitivno razliko glede na obstoječe stanje) na področju informacijske varnosti tudi v organizacijah, ki že imajo vpeljane določene varnostne politike v svoje poslovanje?

S predstavljeno metodologijo smo želeli potrditi tudi drugo raziskovalno vprašanje magistrske naloge. Trdimo, da bo z dosledno vpeljavo vseh izbranih rešitev za odkrite nevarnosti IS, prikazane v desnem stolpcu preglednice 23, dosežena pozitivna razlika glede na obstoječe stanje na področju informacijske varnosti in pretoka informacij tudi v organizaciji, ki je že nosilec uglednega certifikata s področja informacijske varnosti, ISO 27001:2005. Našo trditev dodatno potrjujejo izjave njenih sogovornikov na polstrukturiranem intervjuju. Direktor je dejal, da bodo dobljeni predlogi in rešitve upoštevani pri pripravi nove ocene tveganja, ki jo morajo napraviti za ponovno presojo že pridobljenega certifikata. Presoja se izvaja vsako leto. Predloge ranljivosti IS je označil kot križišče za naslednjih deset novih, ki bodo morda zanemarljivi z dobljenimi. Konceptu je bila pripisana prednost prav v razpršenosti in vključitvi zaposlenih iz celotne organizacije. Pridobljene izkušnje s prvega in drugega srečanja kot tudi ocenjevanja predlogov bodo udeleženci lahko širili naprej na ostale zaposlene. Po proučitvi dobljenih rezultatov in določitvi prioritet bodo vključeni tudi pri vpeljavi rešitev. Te pa bodo imele pozitiven vpliv na obstoječo informacijsko varnost, kar potrjuje naše drugo raziskovalno vprašanje.

5.6 Omejitve in možnosti nadaljnjega raziskovanja

V predstavljeni metodologiji vzamemo za osnovo nabor sedanjih in pretečih groženj ter ranljivosti IS. Od začetne, skrbno premišljene kategorizacije IS in izbire inovativne skupine posameznikov za kreativno sejo možganske nevihte v prvi fazi koncepta je precej odvisno, kakšne rezultate bomo na koncu dobili. To se je potrdilo tudi v našem primeru. Lahko rečemo, da s kategorizacijo nastavimo pogled z lupo nad opazovane informacijske vire, udeleženci seje in njen koordinator pa predstavljajo filter, ki določa, kaj pride skozi. Bolj je skupina inovativna, širše in globlje vidi možne ranljivosti sistema. Tudi dober koordinator seje potrebuje kar nekaj izkušenj in vaje, da skupino usmerja in ustrezno motivira z upoštevanjem pravil metode viharjenja možganov.

Po srečanjih z vodji IT in ostalimi v organizacijah ugotavljamo, da obstaja precej rezerve na področju natančnejše ocenitve škode za predvidene ranljivosti in morebitne grožnje. Pri oceni tveganja bi bilo zato potrebno za vsako grožnjo posebej napraviti natančnejšo cenovno analizo in upoštevati vse možne posledice. Tako bi v organizaciji prišli do osnove za izračun pričakovane letne izgube za posamezno rešitev oz. oportunitetnega stroška, če bi se reševanju posamezne varnostne vrzeli odpovedali.

Med našo raziskavo v obdobju petih mesecev ni bilo mogoče najti nobene zainteresirane organizacije oz. ustanove, ki bi si bila pripravljena za to vzeti čas. V sodelujočih organizacijah pa smo imeli omejene kadrovske in časovne možnosti za delo v skupini. Osnovna metodologija predvideva več skupinskih srečanj, v raziskavi smo se omejili na dve, ki sta bili sprejemljivi s strani sogovornikov v organizacijah. Na tem področju vidimo bistvene omejitve tudi pri nadaljnjem raziskovanju.

V prikazu nove metodologije smo se omejili na prve tri faze novega pristopa oz. metode, ki smo jih zaradi omejenih časovnih in kadrovskih možnosti dela s skupino v organizacijah nekoliko prilagodili (iskanje in ocenjevanje varnostnih vrzeli, iskanje, usklajevanje, ocenjevanje in študija izvedljivosti rešitev za vrzeli, posamični polstrukturirani intervju z vodji IT v organizacijah in kritična analiza dobljenih rezultatov). V celotnem konceptu sta predvideni še fazi izvedbe rešitev in spremljanja učinkov ter sprotne uvedbe morebitnih popravnih ukrepov. To zahteva dobro zasnovano študijo in opazovanje ranljivosti na daljši rok. Pogledati bi morali, kakšno je bilo stanje pred vpeljavo in po vpeljavi te metodologije v organizaciji. Zanimiva bi bila tudi študija, kjer bi izvedli raziskavo s kombiniranjem. Na eni strani bi imeli kontrolno skupino primerljivih organizacij, kjer uporabljajo za varnostni pristop standarde in varnostne politike, nasprotna skupina primerljivih organizacij pa bi uporabila še predlagano metodologijo (Likar in Trček 2012).

Predstavljena inovativna metodologija upravljanja varnosti IS in informacij ni nadomestilo za standardne metode varnosti. Gre za pristop, ki kombinirano dopolnjuje oboje, standarde informacijske varnosti ter inovativno upravljanje varnosti.

6 SKLEP

V raziskavi smo si za cilj postavili preveriti predstavljeno metodologijo povečanja varnosti IS v praksi. Na začetku smo jo nameravali izpeljati v treh naključno izbranih organizacijah. Zaradi vzrokov, podrobneje prikazanih v točki 4.1, smo jo nato izpeljali le v dveh srednje velikih industrijskih organizacijah. Obe sta dejavni na področju visokih tehnologij. Ena je izrazito izvozno usmerjena. Sta uspešni in ustvarjata visoko dodano vrednost.

Na uvodnem srečanju z vodji IT se je izkazalo tudi, da so časovne in kadrovske možnosti dela s skupino omejene, zato smo osnovno metodologijo v drugi in tretji fazi nekoliko prilagodili. Število srečanj skupine smo omejili na dve. S prvo smo na možganski nevihti iskali varnostne vrzeli IS z drugo pa rešitve zanje. Ocenjevanje predlogov vrzeli je potekalo s strani izbranih ocenjevalcev posamično v organizaciji. Četrto, zadnje, srečanje je bilo namenjeno polstrukturiranemu intervjuju z vodji IT oz. predstavniki ožjega vodstva organizacije.

Prikazana metodologija, ki poteka v več fazah in skupinah, zahteva določene človeške vire. Ti so v primerjavi z izgubami, ki jih lahko imamo zaradi ranljivega IS, razmeroma majhni. Po nekaterih izvedenih analizah pri nas je dobrih 9 % vprašanih organizacij potrdilo škodo do 10.000 EUR zaradi kraje informacij, približno 2 % pa med 10.000 in 49.000 EUR (Židanik et al. 2004, 16).

Da bi odgovorili na obe raziskovalni vprašanji magistrske naloge, smo k raziskavi povabili organizacijo, ki na področju varovanja IS odstopa od povprečja. Z drugim raziskovalnim vprašanjem smo skušali potrditi, da nova predstavljena metodologija tudi v taki organizaciji omogoča dobiti pozitivno razliko glede na obstoječe stanje na področju varnosti IS. Potrditev tega vprašanja smo podrobneje analizirali v točki 5.5.

LITERATURA

Anderson, Ross. 2001. *Security engineering: A guide to building dependable distributed systems*. New York: John Wiley & Sons.

Dhillon, Gurpreet. 2001. *Information security management: Global challenges in the new millennium*. London: Idea Group Publishing.

Easterby-Smith, Mark, Richard Thorpe in Andy Lowe. 2005. *Raziskovanje v managementu*. Koper: Fakulteta za management.

Frick, Vaughn in Lill All. 2000. *Ten imperatives for e-business success*. 4. izd. Stamford, CT: Gartner Group.

Greengard, Samuel. 2011. *Šest pogostih napak varnosti IT in kako se jim izogniti*. Ljubljana: Microsoft d.o.o. Http://www.microsoft.com/business/smb/sl-SI/varnost/Izogibanje-pogostih-napak-pri-IT.mspx (27. 2. 2011).

Herold, Rebecca. 2010. *Why information security training and awareness are important*. New York: Auerbach Publications. Http://www.infosectoday.com/Articles/Security_Awareness_Training.htm (13. 2. 2012).

Hinson, Gary. 2003. *Human factors in information security*. Surrey: IsecT Ltd. Http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf (14. 1. 2012).

Hong-li, Liu in Ying-ju Zhu. 2009. *Measuring effectiveness of information security*. New York: IEEE.

InfoSecurityLab, Slovenia. 2012. *Security incident*. Http://webmail.infosum.net/communication/security-incident.html (3. 3. 2012).

International Standards Organization. (ISO) 2005a. *Informacijska tehnologija-Varnostne tehnike-Sistemi za upravljanje varovanja informacij*. Šempeter pri Gorici: Palsit d.o.o. (prevod ISO/IEC 27001:2005 standarda, prva izdaja).

International Standards Organization. (ISO) 2005b. *Informacijska tehnologija-Varnostne tehnike-Kodeks za upravljanje varovanja informacij*. Šempeter pri Gorici: Palsit d.o.o. (prevod ISO/IEC 27002:2005 standarda, druga izdaja).

International Standards Organization. (ISO) 1998. *Information technology - Guidelines for the management of IT security - Part 3: Techniques for the management of IT security*. Http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail. htm? csnumber=21756 (27. 3. 2012).

Likar, Borut. 2002. *Uspeti z idejo:tehnike in metode ustvarjanja, razvoja in trženja idej*. Ljubljana: Korona plus: Pospeševalni center za malo gospodarstvo.

Likar, Borut, Dejan Križaj in Peter Fatur. 2006. *Management inoviranja*. Koper: Fakulteta za management.

Likar, Borut, Cyril Chovan, Peter Fatur, Arne Kullbjer, Silvia Medova in Vassilis Tsaggaris. 2007. *Managing innovation and R&D processes in EU environment*. Ljubljana: Korona plus d.o.o. – Inštitut za inovativnost in tehnologijo.

Likar, Borut, Peter Fatur, Marko Ropret, Denis Trček, Mirko Markič, Cene Bavec, Maja Škafar in Karmen Rodman. 2011. *Referenčni model inoviranja, zaključno poročilo o rezultatih raziskovalnega projekta,* 2. oktober, 204. Koper: Fakulteta za management.

Likar, Borut in Denis Trček. 2012. A methodology for provision of sustainable information systems security. *Cybernetics and Systems* 43 (1): 22-33.

Lipparini, Andrea. 2002. *La gestione strategica del capitale intellettuale e del capitale sociale*. Bologna. Il mulino.

Manik, Dey. 2007. *Information security management - A practical approach*. New York. IEEE.

Ministrstvo za javno upravo (MJU). 2010. *Priporočila informacijske varnostne politike javne uprave.* Http://www.mju.gov.si/si/zakonodaja_in_dokumenti/pomembni_ dokumenti (17. 8. 2011).

National Institute of Standards and Technology (NIST) 2002. *Risk management guide for information technology systems-Recommendations of the National institute of standards and technology*. Http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf (26. 2. 2011).

National Institute of Standards and Technology (NIST) 2006. *Guide to computer security log management-Recommendations of the National institute of standards and technology.* Http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf (19. 4. 2012).

National Institute of Standards and Technology (NIST) 2008. *Computer security incident handling guide-Recommendations of the National institute of standards and technology.* Http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf (23. 4. 2012).

O'Brien, James A. 2004. *Management information systems: managing information technology in the business enterprise*. New York: McGraw-Hill Companies.

Organisation for Economic Co-operation and Development (OECD). 2002. *OECD Guidelines for the security of information systems and networks: Towards a culture of security*. Http://www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html (28. 12. 2011).

Pečjak, Vid. 1989. *Poti do idej: Tehnike ustvarjalnega mišljenja v podjetjih, šolah in drugje*. Ljubljana: Samozaložba.

Peltier, Thomas R. 2005. *Implementing an information security awareness program*. Http://www.infosectoday.com/IT%20Today/Peltier_awareness.pdf (13. 2. 2012).

Purser, Steve. 2004a. *Integrating security into the corporate culture*. Http://www.infosecwriters.com/text_resources/pdf/integrating.pdf (15. 1. 2012).

Purser, Steve. 2004b. *Managing information security in modern commercial environments*. Http://www.infosecwriters.com/texts.php?op=display&id=199/Commercial_Managing_Information_Security-2.pdf (15. 1. 2012).

Purser, Steve. 2004c. *10 communications tips for security managers*. Http://www.infosecwriters.com/text_resources/pdf/Communication_For_Security_Managers.pdf (21. 1. 2012).

Rainer, R. Kelly, Efraim Turban in Richard E. Potter. 2007. *Introduction to information systems: Supporting and transforming business*. New York: John Wiley & Sons.

Sarbanes–Oxley Act 2002. *Public law 107–204*. Http://www.google.si/url?sa=t&rct=j&q=sarbanes-oxley%20act%20of%202002&source=web&cd=2&ved=0CEAQFjAB&url=http%3A%2F%2Fnews.findlaw.com%2Fcnn%2Fdocs%2Fgwbush%2Fsarbanesoxley072302.pdf&ei=i4aOT7vfJIf3sgaSvuScCQ&usg=AFQjCNHPpY4dwu-GUPLnrtolFYm1i-E6Ww&cad=rja (18. 4. 2012).

Schneier, Bruce. 2000. *Secrets and lies: Digital security in a networked world.* New York: John Wiley & Sons.

Smart Com, d.o.o. 2012. *Varnostno preverjanje ranljivosti IS*. Http://www.smart-com.si/uploads/datoteke/varnostno_preverjanje_ranljivosti_is.pdf (3. 3. 2012).

Stefanek, George. 2002. *Information security best practices 205 basic rules*. Woburn, MA: Butterworth-Heinemann.

Trček, Denis. 2006. *Managing information systems security and privacy*. Berlin/Heidelberg: Springer.

Vidmar, Tone. 2002. *Informacijsko-komunikacijski sistem*. Ljubljana: Pasadena.

Židanik, Marjan, Aleksander Šinigoj, Marko Pahor in Miroslav Kranjc. 2004. *Raziskava o informacijski varnosti – RIV 2004*. Šempeter pri Gorici: Inštitut za informacijsko varnost.

PRAVNI VIRI

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1). *Uradni list RS*, št. 94/2007.

Zakon o Informacijskem pooblaščencu (ZInfP). *Uradni list RS*, št. 113/2005.

PRILOGE

Predvideni plan raziskave

Naslov mag. naloge:
INOVATIVNI PRISTOP PRI ZAGOTAVLJANJU VARNOSTI INFORMACIJSKIH SISTEMOV

Potek raziskave:

a) predvideva se dve (2) skupinski in eno (1) posamično srečanje. Prvo s skupino vsaj pet (5) zaposlenih, drugo s skupino pet (5) ali več zaposlenih (del udeležencev je lahko tudi iz prve skupine). Zaželeno je, da sta vključena oba spola, različnih starosti, iz različnih oddelkov in nivojev institucije. Tretje srečanje predstavlja polstrukturirani intervju z vodjem službe za informatiko oz. specialistom informacijske varnosti obravnavane ustanove oz. organizacije;

b) ime ustanove oz. organizacije v nalogi ne bo nikjer izpostavljeno. Znano bo avtorju naloge in mentorju;

c) če bo vodstvo ustanove oz. organizacije menilo za potrebno, se lahko podpiše tudi ustrezen zavezujoč dokument glede varovanja informacij.

1. SREČANJE
S skupino ustvarjalnih posameznikov (5 oseb, lahko pa tudi več) izmed zaposlenih bomo z inovativno tehniko (metoda viharjenja možganov) skušali identificirati:

- *najbolj pereče aktualne (sedanje) varnostne pomanjkljivosti obstoječega IS;*
- *potencialne varnostne vrzeli informacijskega sistema (IS) v bodočnosti;*
- *možne varnostne grožnje.*

Vključene so lahko tudi *kulturne posebnosti ustanove oz. organizacije* (predvidoma 40 minut do 1 ure).

Varnostni specialist ali vodja službe za informatiko iz organizacije ali ustanove najprej v stavku, dveh, predstavi trenutno stanje ravni informacijske varnosti iz tehničnega in organizacijskega vidika. Pomembno je, da je ta uvod le na konceptualni ravni. Izogibanje podrobnim pojasnilom je namerno, da se prepreči tudi ne-IT udeležencem, da se vključijo v to mentalno shemo kot strokovnjaki na tem področju. Je pa pomembno, da osnovne pojme informacijske varnosti jasno razumejo udeleženci skupine.

Moderator srečanja (avtor mag. naloge) bo skupini zastavljal vprašanja, ki bodo zadevala informacijsko varnost petih za organizacijo oz. ustanovo najpomembneje kategoriziranih informacijskih virov (Priloga). Predlagane ideje bo sproti zapisoval na velik kos papirja, formata B0, tako da bodo vidne vsem udeležencem in bo mogoče navezovati nove ideje tudi na predhodne. Dobljene rezultate bo avtor mag. naloge v prepisani (elektronski v obliki preglednice) posredoval kontaktni osebi, ki je sodelovala pri organizaciji srečanja. Dodan bo tudi ocenjevalni obrazec (ki vam ga za boljšo predstavo pošiljam v prilogi). Rezultate prve skupine, skupaj z ocenjevalnim obrazcem, naj bi prejel vsak od izbranih kandidatov (ocenjevalcev) bodočega, drugega, srečanja (5 kandidatov ali več).

Priloga 1

Pri ocenjevanju naj bi sodelovali poznavalci svojega ožjega področja (programerji računalniških rešitev, sodelavci iz finančne, kadrovske službe, IT podpore, raziskovalci, razvijalci, varnostnik itd.). Vsak ocenjevalec naj bi intuitivno izbral 5-7 zanj najpomembnejših varnostnih pomanjkljivosti (vrzeli). Ocenjevanje se na ta način časovno do dogovorjenega drugega srečanja izvede, kot posameznikom najbolje ustreza. Kontaktna oseba v organizaciji oz. ustanovi po končanem ocenjevanju zbere ocenjevalne obrazce in jih pošlje avtorju mag. naloge v dogovorjeni obliki (časovno gledano najbolje v priponki po e-pošti, preslikane ali fotografirane z mobilnikom). Lahko pa se prevzamejo tudi originali osebno s strani avtorja. Dobljeni rezultati ocenjevanja bodo ustrezno razvrščeni in služijo kot osnova za drugo srečanje s skupino.

2. SREČANJE
To srečanje bo sledilo prvemu po preteku nekaj dni (v skladu z dogovorom in razpoložljivostjo zaposlenih). Trajalo naj bi eno šolsko uro. Skupino naj bi sestavljalo vsaj 5 zaposlenih ali več. Med njimi naj bi bili tisti, ki so ocenjevali rezultate prve skupine. V skupini so lahko tudi posamezniki, ki so že bili na prvem srečanju. Drugo srečanje daje poudarek iskanju možnih rešitev za ocenjene in razvrščene pomanjkljivosti. Do zaključka srečanja naj bi skupina zbrala rešitve za pet tistih pomanjkljivosti IS, ki so bile ugotovljene kot najpomembnejše oz. najnujnejše, da se jih reši.

V magistrskem delu bomo skušali odgovoriti na dve raziskovalni vprašanji. Eno med njima je, da nam bo s predlagano metodologijo z zaposlenimi uspelo poiskati in izbrati rešitve za varnostne pomanjkljivosti IS, ki lahko prispevajo k izboljšanju varnosti obstoječega IS in pretoka informacij.

3. SREČANJE
Predstavlja *posamični polstrukturirani intervju*, ki ga bomo izpeljali z vodjo IT oddelka oz. strokovnjakom za informacijsko varnost, če to mesto v organizaciji obstaja (pribl. 45 minut).

Kaj dobi ustanova oz. organizacija?

- izvedeno tehniko, neposredne rezultate možganske nevihte prvega srečanja in tri končne predloge za izboljšanje varnosti njihovega IS;
- rezultate končne analize mag. naloge.

Predstavljena inovativna metodologija upravljanja varnosti IS in informacij ni nadomestilo za standardne metode varnosti. Gre za pristop, ki kombinirano dopolnjuje oboje, standarde informacijske varnosti ter inovativno upravljanje varnosti.

Moji osebni podatki: _____

Naslov: _____

Mobil. tel.: _____

E-naslov: _____

Kategorizacija virov IS

Kategorija	**Opis vrste vira**
Informacijski viri	□ Dokumentacijski podatki □ Podatkovne baze □ Elektronska sporočila □ Ostale datoteke **Upoštevajte vse medije (papir, mikrofilmi, trdi disk)**
Programska oprema	□ Operacijski sistemi □ Uporabniška programska oprema □ Komunikacijska programska oprema
Aparaturna oprema	□ Strežniki □ Stacionarni in prenosni računalniki □ Komunikacijska stikala □ Tiskalniki
Elementi infrastrukture	□ Klimatske naprave □ Sistemi za neprekinjeno napajanje (UPS)
Splošni viri	□ Poslovni prostori □ Pisarniška oprema □ Produkti in storitve organizacije
Osebje in neopredmeteni viri	□ Zaposleni □ Poslovni partnerji □ Ugled pri potrošniških organizacijah □ Zaščitne znamke, patenti □ Tržni delež
Dodatno	□ _____ □ _____ □ _____

Opombe: - s križcem (**x**) naj se označi za organizacijo pomembne informacijske vire;
- pred petimi najpomembnejšimi naj se dopiše številke (št. 1 je najpomembnejši vir).

Ocenjevalni obrazec

OCENJEVANJE PREDLOGOV

1.) Intuitivno izberite 5-7 boljših predlogov varnostnih vrzeli

Zaporedna številka predloga vrzeli

2.) Ocenjevanje treh izbranih predlogov vrzeli iz točke 1

Tri (3) predloge vrzeli iz točke 1, ki jim pripisujete največji pomen, vpišite v spodnjo preglednico in jih ocenite z vrednostno oceno od 1 do 5 (5 je najbolj pomemben).

Številka predloga vrzeli (iz točke 1)	**K*** Kriterij pomembnosti (ocena od 1-5)

* S kriterijem se ocenjuje pomembnost oz. aktualnost predloga vrzeli za informacijsko varnost.

Oddelek, iz katerega prihaja ocenjevalec:

_____

Obrazec SWOT

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)

Predlog vrzeli: _____

Analiza SWOT ocenjenih predlogov vrzeli št. 2 in 3 (1. org.)

S (Prednosti /Strengths/) ● odpadejo stroški za ureditev rezervne lokacije; ● odpadejo stroški in čas zaposlenega(ih), ki skrbi(jo) za urejanje papirnega gradiva; ● ni stroškov za arhivske regale in protipožarne omare; ● odpadejo stroški vlaganja v pridobivanje tehničnega znanja in tehnologijo arhiviranja.	**W (**Slabosti /Weaknesses/) ● zamudno iskanje gradiva v papirni in elektronski obliki; ● otežena obnova ali celo izguba podatkov (slepi backup) po odpovedi hardvera strežnika (okvara diskovnega krmilnika); ● nižja bonitetna ocena pri potencialnih bodočih partnerjih; ● slabše možnosti pri pridobivanju projektov na mednarodnih razpisih.
O (Priložnosti /Opportunities/) ● ureditev struge reke v neposredni bližini objekta organizacije s strani občine in države; ● ponudbe zunanjih kvalificiranih ponudnikov arhiviranja (Pošta Slovenije ipd.) na trgu; ● davčne vzpodbude dviga standardov poslovanja poslovnih subjektov s strani države; ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001.	**T (**Nevarnosti /Threats/) ● sprememba pogojev zavarovanja objekta organizacije s strani zavarovalnice; ● požar, potres, zaradi bližine reke tudi zalitje z vodo; ● dvig standardov pri pridobivanju nepovratnih sredstev s strani države; ● vstop novega močnega konkurenta na trg.

Slika 1: SWOT analiza predloga vrzeli neurejen arhiv

S (Prednosti /Strengths/) ● delo na daljavo za uporabnike, ki to potrebujejo; ● 24/7 dostop do notranjega omrežja; ● geografska neodvisnost; ● manjši stroški prevoza in ureditve del. mesta, če je zaposlenemu omogočeno tri dni v tednu opravljati delo na domu.	**W (**Slabosti /Weaknesses/) ● ažurni seznam večjega števila upravičencev tega dostopa; ● zasedene datoteke na sistemu medtem ko se izvaja zaščitno kopiranje na tračno enoto (prijave izven delovnega časa); ● hitrost dostopa do prijave in podatkov, če tehnologija ni sodobna; ● večja ranljivost sistema.
O (Priložnosti /Opportunities/) ● ponudba tovrstne zmogljive opreme na trgu; ● prevzem organizacije s strani konkurenta kjer je tovrstni dostop že doslej dobro pokrit (delo na domu); ● liberalizacija trga držav, proizvajalk te specialne opreme; ● posodobljena infrastruktura lokalnega ponudnika telekomunikacijskih storitev.	**T (**Nevarnosti /Threats/) ● vdor v omrežje (kraja ali zloraba podatkov); ● možnost vnosa računalniškega virusa iz oddaljene delovne postaje; ● povišanje davkov in s tem dražja nova oprema; ● sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice.

Slika 2: SWOT analiza predloga vrzeli VPN dostopi do omrežja organizacije

Priloga 5

Analiza SWOT ocenjenih predlogov vrzeli št. 4 in 5 (1. org.)

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● prihranek časa sistemskega inženirja za administracijo pozabljenih gesel; ● enostaven dostop do uporabniškega imena sodelavca v primeru nadomeščanja; ● odpade deponiranje gesel v kuvertah tajništva ali vodje oddelka; ● hitrejši dostop do delovne postaje.	● kršenje interne varnostne politike; ● nepreglednost aktivnih uporabnikov na sistemu (prijava v imenu drugega); ● večja ranljivost sistema; ● dostop do tujega elektronskega predala.
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● privzeta nastavitev preverjanja moči gesla zunanjega skrbnika sistema; ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● upoštevanje varnostne politike partnerja s katerim organizacija poslovno sodeluje; ● zavezujoč pravilnik združenja v katerem je organizacija.	● nepooblaščeni dostopi do posameznih del. postaj v času odsotnosti uporabnikov; ● dostop do uporabniških programov v imenu drugega uporabnika preko VPN povezave; ● z zlorabo uporabniškega imena in gesla se na sistemu izvede postopek, ki ima lahko finančne posledice; ● dostop do zaupnih dokumentov.

Slika 3: SWOT analiza predloga vrzeli uganljiva standardna gesla

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● izpeljava določenega opravila v zares izrednih razmerah; ● delovni proces se lahko neovirano nadaljuje; ● prihranek stroškov skladiščenja (npr. pošiljke na pošti); ● osvajanje delovnih veščin zaposlenega, ki se nadomešča.	● ključno osebo je težko nadomestiti 100 %; ● večja možnost napak; ● preobremenjenost zaposlenih ki poleg svojih dnevnih opravil opravljajo še nadomeščanje; ● možen vpogled v zasebne podatke na profilu uporabnika, ki se ga nadomešča.
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● nadomeščanje skladno z varnostno politiko partnerja, s katerim organizacija poslovno sodeluje; ● ugodne ponudbe izobraževanj uporabnikov s področij, ki so predmet nadomeščanja; ● preventivna zdravstvena politika države.	● s pravicami odsotnega uporabnika se po pomoti sproži neželjen postopek; ● dostop odhajajočega zaposlenega do zaupnih dokumentov; ● s pravicami odsotnega uporabnika se lahko dostopa do ostalih delovnih postaj; ● nepreverjene privzete nastavitve na sistemu.

Slika 4: SWOT analiza predloga vrzeli nadomeščanje v času odsotnosti

Analiza SWOT ocenjenih predlogov vrzeli št. 6 in 7 (1. org.)

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● delo na domu; ● odpade strošek nabave prenosnika, ki je lahko boniteta delavcu za uspešnost pri delu; ● večja pripadnost organizaciji; ● veščine, pridobljene za privatne zadeve, se lahko s pridom uporabijo tudi za službene.	● administratorska pooblastila na uporabniškem profilu zaradi značaja službenih prog. rešitev (delujejo le v tem načinu); ● večja možnost vnosa virusa na operacijski sistem (priklop na različna zunanja omrežja); ● možnost fizičnih poškodb zaradi pogostega prenašanja; ● večja možnost odtujitve.
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● varnostna politika partnerja, s katerim organizacija poslovno sodeluje, to omogoča; ● ponudba učinkovitih možnosti kriptiranja podatkov na trgu; ● partnerstvo z organizacijo, ki trži protivirusne programske rešitve.	● zloraba lokalnih podatkov v primeru odtujitve; ● možnost vnosa računalniškega virusa; ● požar na domu; ● dostop otrok do delovne postaje.

Slika 5: SWOT analiza predloga vrzeli uporabe prenosnikov za privatne zadeve

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● odpade čas zaposlenega(ih), ki skrbi(jo) za urejanje osnovnih sredstev; ● odpadejo stroški vlaganja v pridobivanje znanja in tehnologijo popisa osn. sredstev; ● lažji prenos osnovnih sredstev med različnimi lokacijami organizacije; ● prihranek potnih stroškov za popis oddaljenih lokacij organizacije.	● neurejeno stanje osnovnih sredstev v organizaciji; ● negativni vpliv na pripravo letnega proračuna za nabavo nove opreme in amortizacijo osnovnih sredstev v produkciji; ● prikazovanje neažurnega stanja osnovnih sredstev ima vpliv na ostale izračune; ● otežena prijava policiji po odtujitvi sredstev (manjkajoče serijske številke).
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● ponudba številnih prog. rešitev na trgu za delo z osnovnimi sredstvi ob uporabi črtne kode; ● prevzem organizacije s strani konkurenta, za katerega to storitev izvaja zunanja org.; ● sprememba zakonodaje; ● davčne vzpodbude za nakup pametnih čitalcev osnovnih sredstev.	● sprejem restriktivnejše zakonodaje glede zajema osnovnih sredstev gospodarskih subjektov; ● zaradi neurejenega stanja slabša bonitetna ocena organizacije; ● problem pri uveljavljanju garancij pri prodajalcu opreme; ● sprememba pogojev zavarovalnice pri zavarovanju opreme.

Slika 6: SWOT analiza predloga vrzeli osnovnih virov

Priloga 5

Analiza SWOT ocenjenega predloga vrzeli št. 8 (1. org.)

S (Prednosti /Strengths/) ● manjša poraba električne energije; ● ni problema z aktivnimi povezavami pri zaščitnem kopiranju podatkov; ● med delovnim časom so aktivne le delovne postaje prisotnih zaposlenih; ● manjša verjetnost požara zaradi pregrevanja.	**W (**Slabosti /Weaknesses/) ● dnevna poraba časa za zagon in spuščanje operacijskega sistema; ● večja verjetnost odpovedi vrtljivih delov (diski, ventilatorji); ● nedostopnost v primeru dnevnega posodabljanja protivirusne zaščite; ● nedostopnost preko VPN povezave izven delovnega časa.
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● obdobja pomanjkanja el. energije (redukcije); ● poostrena okoljska zakonodaja glede porabe električne energije; ● podražitev električne energije.	**T (**Nevarnosti /Threats/) ● pregrevanje delovne postaje v okvari (potencialni vir požara); ● oddaljeni dostop do vključene delovne postaje s strani nepooblaščenih uporabnikov; ● sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice; ● udari strele in prenapetostne motnje.

Slika 7: SWOT analiza predloga vrzeli izklapljanja delovnih postaj

Preglednica 1: Povzetek treh bistvenih kriterijev SWOT ocen za razvrščanje ocenjenih varnostnih vrzeli (1. org.)

Vrstni red	Ime predloga vrzeli	Nevarnosti	Slabosti	Priložnosti
1	Dostop do ERP sistema	Zavračanje faktur s strani kupcev ali dobaviteljev Zmanjšanje naročil kupcev Negativni vpliv na ugled organizacije Zaostritev pogojev OEM sodelovanja s strani naročnika	Otežena presojna sled na sistemu (kdo, kdaj, kaj) v primeru da ni vključenega sledenja na bazi (auditing) Večja verjetnost napak na finančnih planskih in ostalih podatkih Možen nepooblaščen dostop do ostalih modulov ERP sistema Nepooblaščeno izvajanje kalkulacij na planskih podatkih negativno vpliva na storilnost sistema Večje tveganje z vidika varnosti	Ponudba licenc pogodbenega partnerja pod ugodnejšimi pogoji Promocijska ponudba šolanj ERP sistema s strani pogodbenega partnerja Prihod ugodnejšega ponudnika ERP sistema na notrani trg Ugodnejša davčna zakonodaja na področju vlaganj v posodobitev poslovanja
2	Neurejen arhiv	Sprememba pogojev zavarovanja objekta organizacije s strani zavarovalnice Požar, potres, zaradi bližine reke tudi zalitje z vodo Dvig standardov pri pridobivanju nepovratnih sredstev s strani države Vstop novega močnega konkurenta na trg	Zamudno iskanje gradiva v papirni in elektronski obliki Otežena obnova ali celo izguba podatkov (slepi backup) po odpovedi hardvera strežnika (okvara diskovnega krmilnika) Nižja bonitetna ocena pri potencialnih bodočih partnerjih Slabše možnosti pri pridobivanju projektov na mednarodnih razpisih	Odpadejo stroški za ureditev rezervne lokacije Odpadejo stroški in čas zaposlenega(ih), ki skrbi(jo) za urejanje papirnega gradiva Ni stroškov za arhivske regale in protipožarne omare Odpadejo stroški vlaganja v pridobivanje tehničnega znanja in tehnologijo arhiviranja
3	VPN dostopi do omrežja organizacije	Vdor v omrežje (kraja ali zloraba podatkov) Možnost vnosa računalniškega virusa iz oddaljene delovne postaje Povišanje davkov in s tem dražja nova oprema Sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice	Ažurni seznam večjega števila upravičencev tega dostopa Zasedene datoteke na sistemu medtem ko se izvaja zaščitno kopiranje na tračno enoto Hitrost dostopa do prijave in podatkov, če tehnologija ni sodobna Večja ranljivost sistema	Ponudba tovrstne zmoglj. opreme na trgu Prevzem organizacije s strani konkurenta kjer je tovrstni dostop že doslej dobro pokrit (delo na domu) Liberalizacija trga držav, proizvajalk te specialne opreme Posodobljena infrastr. lokalnega ponudnika telekomunikacijskih storitev
4	Uganljiva standardna gesla	Nepooblaščeni dostopi do posameznih del. postaj v času odsotnosti uporabnikov Dostop do programskih rešitev v imenu drugega uporabnika preko VPN povezave Z zlorabo uporabniškega imena in gesla se na sistemu izvede postopek, ki ima lahko finančne posledice Dostop do zaupnih dokumentov	Kršenje interne varnostne politike Nepreglednost aktivnih uporabnikov na sistemu (prijava v drugem imenu) Večja ranljivost sistema Dostop do tujega elektronskega predala	Privzeta nastavitev preverjanja moči gesla zunanjega skrbnika sistema Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Upoštevanje varnostne politike partnerja s katerim organizacija poslovno sodeluje Zavezujoč pravilnik združ., v katerem je org.

Priloga 5

Vrstni red	Ime predloga vrzeli	Nevarnosti	Slabosti	Priložnosti
5	Nadomeščanje v času odsotnosti	S pravicami odsotnega uporabnika se po pomoti sproži neželjen postopek Dostop odhajajočega zaposlenega do zaupnih dokumentov S pravicami odsotnega uporabnika se lahko dostopa do ostalih delovnih postaj Nepreverjene privzete nastavitve na sistemu	Ključno osebo je težko nadomestiti 100 % Večja možnost napak Preobremenjenost zaposlenih ki poleg svojih dnevnih opravil opravljajo še nadomeščanje Možen vpogled v zasebne podatke na profilu uporabnika, ki se ga nadomešča	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Nadomeščanje skladno z varnostno politiko partnerja s katerim organizacija poslovno sodeluje Ugodne ponudbe izobraževanj uporabn. s področij, ki so predmet nadomeščanja Preventivna zdravstvena politika države
6	Uporaba prenosnikov za privatne zadeve	Zloraba lokalnih podatkov v primeru odtujitve Možnost vnosa računalniškega virusa Požar na domu Dostop otrok do delovne postaje	Administratorska pooblastila na uporabniškem profilu zaradi značaja službenih prog. rešitev (delujejo le v tem načinu) Večja možnost vnosa virusa na operacijski sistem (priklop na različna zunanja omrežja) Možnost fizičnih poškodb zaradi pogostega prenašanja Večja možnost odtujitve	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Varnostna politika partnerja, s katerim organizacija poslovno sodeluje, to omogoča Ponudba učinkovitih možnosti kriptiranja podatkov na trgu Partnerstvo z org., ki trži protivirusne programske rešitve
7	Osnovni viri (evidence, na terenu, reverzi)	Sprejem restriktivnejše zakonodaje glede zajema osnovnih virov gospodarskih subjektov Zaradi neurejenega stanja slabša bonitetna ocena organizacije Problem pri uveljavljanju garancij pri prodajalcu opreme Sprememba pogojev zavarovalnice pri zavarovanju opreme	Neurejeno stanje osnovnih virov v organizaciji Negativni vpliv na pripravo letnega proračuna za nabavo nove opreme in amortizacijo osnovnih virov v produkciji Prikazovanje neažurnega stanja osnovnih virov ima vpliv na ostale izračune Otežena prijava policiji po odtujitvi sredstev (manjkajoče serijske številke)	Ponudba številnih prog. rešitev na trgu za delo z osnovnimi viri ob uporabi črtne kode Prevzem organizacije s strani konkurenta, za katerega to storitev izvaja zunanja org. Sprememba zakonodaje Davčne vzpodbude za nakup pametnih čitalcev osnovnih virov
8	Izklapljanje delovnih postaj	Pregrevanje delovne postaje v okvari (potencialni vir požara) Oddaljeni dostop do vključene delovne postaje s strani nepooblaščenih uporabnikov Sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice Udari strele in prenapetostne motnje	Dnevna poraba časa za zagon in spuščanje operacijskega sistema Večja verjetnost odpovedi vrtljivih delov (diski, ventilatorji) Nedostopnost v primeru dnevnega posodabljanja protivirusne zaščite Nedostopnost preko VPN povezave izven delovnega časa	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Obdobja pomanjkanja el. energije (redukcije) Poostrena okoljska zakonodaja glede porabe električne energije Podražitev električne energije

Analiza SWOT ocenjenih predlogov vrzeli št. 2 in 3 (2. org.)

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● elementi omrežja so nastavljeni v skladu s sprejeto varnostno politiko; ● manjša možnost nepooblaščenega vdora v sistem; ● optimalni izkoristek prenosa podatkov na posameznih segmentih omrežja; ● zaradi varnosti in hitrosti prenosa so izbrani le določeni protokoli in vrata.	● varnostni element (požarni zid) lahko postane ozko grlo za internetni prenos podatkov; ● poraba delovnega časa za posodabljanje in nastavitve; ● tečaji za IT specialiste so dragi; ● stalno spremljanje posodobitev proizvajalca in spletnih forumov IT specialistov.
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● prevzem organizacije s strani konkurenta, ki ima vpeljan standard ISO 27001; ● ugodne ponudbe nadaljevalnih tečajev za sistemske administratorje; ● ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo specialne opreme (outsource); ● promocijske cene novih modelov opreme, z naprednejšimi možnostmi administracije.	● nepreverjene privzete nastavitve; ● odprte možnosti, ki jih je mogoče zlorabiti za dostop do internega omrežja; ● fluktuacija zaposlenih na IT oddelku; ● ukinitev šolanj administratorjem IT zaradi varčevalne politike vodstva.

Slika 1: SWOT analiza predloga vrzeli pravilne konfiguracije varnostnih elementov omrežja

S (Prednosti /Strengths/)	**W (**Slabosti /Weaknesses/)
● znanje je na voljo ostalim v organizaciji; ● lažja zamenljivost zaposlenih v primeru odsotnosti ali izrednih razmer; ● znanje ostane v podjetju, tudi če zaposleni zapusti organizacijo; ● možnosti dodatnega nagrajevanja s spodbujanjem dajanja predlogov; ● vpliv na pozitivno klimo in timsko delo v organizaciji.	● dodatna poraba delovnega časa zaposlenih; ● podatki strukturiranega znanja (recepture, postopki itd.), ki lahko predstavljajo konkurenčno prednost, lahko z zlorabo pridejo do konkurence; ● če podatki niso strukturirani po dogovorjenem sistemu in pregledani ter usklajeni z vodji, nimajo posebne uporabne vrednosti;
O (Priložnosti /Opportunities/)	**T (**Nevarnosti /Threats/)
● fluktuacija kadra na izpostavljenih mestih v proizvodnji in razvoju programske opreme; ● široka ponudba programske opreme za strukturirano shranjevanje znanja zaposlenih; ● prevzem organizacije s strani konkurenta kjer je dokumentiranje znanja že dobro vpeljano; ● povezovanje pretoka znanja z inštituti in nevladnimi organizacijami.	● posredovanje podatkov interne "Wiki baze" konkurenci; ● nestimulativna nagrajevalna politika in slaba klima med zaposlenimi v organizaciji; ● pogosto menjavanje vodstvenega kadra organizacije in spreminjanje prioritet ter strategij; ● preobremenjenost zaposlenih.

Slika 2: SWOT analiza predloga vrzeli strukturni kapital

Priloga 6

Analiza SWOT ocenjenih predlogov vrzeli št. 4 in 5 (2. org.)

S (Prednosti /Strengths/) ● dopolnitev internega pravilnika in ozaveščanje imetnikov teh računalnikov glede varnostne politike, ki zanje velja; ● uporabnik dobi nov prenosni računalnik.	**W (**Slabosti /Weaknesses/) ● materialna škoda; ● izguba uporabnikovih podatkov; ● možna zloraba podatkov; ● izgubljeni čas, ko se vzpostavlja novi sistem (ponovne instalacije in vzpostavitev delovnega okolja).
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● ponudba učinkovitih možnosti kriptiranja nosilcev podatkov na trgu; ● sprememba pogojev zavarovanja prenosne računalniške opreme s strani zavarovalnice; ● ponudba dodatne zaščite nosilcev podatkov na nivoju hardvera.	**T (**Nevarnosti /Threats/) ● odtujitev in mogoča zloraba podatkov; ● otežena prijava policiji po odtujitvi sredstva (manjkajoča serijska številka); ● sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice; ● dostop do strateških dokumentov, če gre za prenosnik zaposlenega iz vodstva.

Slika 3: SWOT analiza predloga vrzeli kraje prenosnika, medijev USB

S (Prednosti /Strengths/) ● redno sledenje spremembam (virusni vdori); ● pridobitev ugleda pri proizvajalcu, če je podjetje tisto, ki je odkrilo morebitno vrzel na programski opremi; ● manjša možnost nepooblaščenega vdora v interni komunikacijski sistem; ● dosledno izpolnjevanje dogovorjene varnostne politike.	**W (**Slabosti /Weaknesses/) ● dodatna poraba delovnega časa sistemskega administratorja; ● stalno spremljanje informacij in opozoril proizvajalca ter spletnih forumov IT specialistov.
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● novi modeli opreme na trgu z zadnjimi verzijami internega programja; ● ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo specialne opreme (outsource); ● ugodne ponudbe nadaljevalnih tečajev za sistemske administratorje.	**T (**Nevarnosti /Threats/) ● instalacija beta popravka (po pomoti) in možni stranski učinki; ● fluktuacija zaposlenih na IT oddelku; ● ukinitev šolanj administratorjem IT zaradi varčevalne politike vodstva; ● neažuriranje dokumentacije nastavitev po zadnjih večjih posegih na konfiguraciji omrežja.

Slika 4: SWOT analiza predloga spremljanja vrzeli na komunikacijski opremi

Analiza SWOT ocenjenih predlogov vrzeli št. 6 in 7 (2. org.)

S (Prednosti /Strengths/) ● hitra rešitev opravila v primeru da določena oseba, ki sicer to opravilo izvaja, manjka; ● razkritje takega primera zahteva od nadrejenih seznanitev uporabnikov, da svojega gesla v nobenem primeru ne posodijo nikomur; ● razkritje primera je vzvod za dopolnitev internega pravilnika o varovanju podatkov.	**W (**Slabosti /Weaknesses/) ● kršenje varnostne politike; ● nepreglednost aktivnih uporabnikov na sistemu (prijava v imenu drugega); ● večja ranljivost sistema; ● dostop do tujega elektronskega predala.
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● upoštevanje varnostne politike partnerja, s katerim organizacija poslovno sodeluje; ● zavezujoč pravilnik združenja, v katerem je organizacija; ● programski vmesniki dostopa do sistema, ki fizično preverjajo uporabnika (prstni odtis).	**T (**Nevarnosti /Threats/) ● uporabniško ime in geslo lahko prideta do nepooblaščenih; ● z zlorabo uporabniškega imena in gesla se na sistemu izvede določeno akcijo, ki ima za organizacijo škodne posledice; ● dostop do zaupnih dokumentov.; ● nepooblaščen dostop do delovne postaje v času odsotnosti uporabnikov.

Slika 5: SWOT analiza predloga pridobitve uporabniškega imena in gesla

S (Prednosti /Strengths/) ● razkritje primera povzroči dopolnitev internega pravilnika o varovanju podatkov.	**W (**Slabosti /Weaknesses/) ● kršenje interne varnostne politike; ● možnost odtujitve najdenega izpisa; ● zloraba podatkov izpisa v privatne namene ali škodo organizacije; ● neprijetnosti v primeru da izpis izgine, in iskanje krivca.
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● upoštevanje varnostne politike partnerja, s katerim organizacija poslovno sodeluje; ● ponudba tiskalnikov, kjer se uporabnik mora identificirati s službeno kartico, preden natisne dokumet iz tiskalniške vrste; ● razkritje primera je vzvod za dopolnitev internega pravilnika o varovanju podatkov.	**T (**Nevarnosti /Threats/) ● vpogled nepooblaščenih oseb v zaupni dokument; ● posredovanje podatkov z najdenega izpisa (nezadovoljni zaposleni) konkurenci; ● odtujitev najdenega izpisa; ● slabši izhodiščni položaj na pogajanjih, če je prišlo do razkritja vsebine dokumenta konkurenci.

Slika 6: SWOT analiza predloga natisnjenih dokumentov na tiskalniku

Priloga 6

Analiza SWOT ocenjenega predloga vrzeli št. 8 (2. org.)

S (Prednosti /Strengths/) ● v primeru požara sistem učinkovito zaduši ogenj; ● uporaba in obvladovanje napredne tehnologije; ● manjše tveganje, da se požar razširi do ostalih prostorov.	**W (**Slabosti /Weaknesses/) ● možne poškodbe na aparaturni opremi; ● nedelovanje poškodovanih strežnikov v času obnove in servisa; ● možnost izgube podatkov delovnega dne; ● nadurno delo zaposlenih v IT oddelku.
O (Priložnosti /Opportunities/) ● prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001; ● ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo IT (outsource); ● upoštevanje varnostne politike partnerja, s katerim organizacija poslovno sodeluje; ● novi modeli opreme z dodatno varnostno zaščito.	**T (**Nevarnosti /Threats/) ● samodejni vklop vgrajenega sistema gašenja s prahom (spontano, el. prehodni pojav); ● zaostritev pogojev zavarovanja opreme organizacije s strani zavarovalnice; ● poškodovanje občutljive IT opreme v sistemskem prostoru; ● gospodarska škoda zaradi nedelujočega sistema.

Slika 7: SWOT analiza predloga sistemski prostor (sistem zavarovanja)

Preglednica 1: Povzetek treh bistvenih kriterijev SWOT ocen za razvrščanje ocenjenih varnostnih vrzeli (2. org.)

Vrstni red	Ime predloga vrzeli	Nevarnosti	Slabosti	Priložnosti
1	Pametni telefoni	Možnost kraje na javnih mestih Prestrezanje podatkov na brezžičnih javnih in brezplačnih omrežjih (hoteli, knjižnice, internetne kavarne) Izpostavljenost direktnemu soncu na delovnem mestu v času odsotnosti zaposlenega Razvoj virusne programske kode na tabličnih operacijskih sistemih Favoriziranje monopolnega ponudnika podatkovnega prenosa in internetnih stotitev ter posledično višja cena	Treba je paziti na baterijo, da je dovolj polna Različni vmesniki za priklop polnilnika v tujini (ZDA, Velika Britanija) Uporabnik je pod nadzorom, kje se giblje (GSM cona) Privzete nastavitve Slabša vidljivost zaslona na dotik na prostem (sonce) Proženje storitve po pomoti ob dotiku napačne ikone na zaslonu	Novi modeli z dodatnimi funkcijami, ki jih ponuja trg Aneksi k podaljšanju naročniških pogodb, ki omogočajo cenovno ugodno menjavo za novejše modele Večje število ponudnikov mobilnih storitev z možnostjo izbire najugodnejšega za podatkovni prenos Modeli 3. generacije tablic z Wi-Fi dostopom in možnostjo telefona
2	Pravilna konfiguracija varnostnih elementov omrežja	Nepreverjene privzete nastavitve Odprte možnosti, ki jih je mogoče zlorabiti za dostop do internega omrežja Fluktuacija zaposlenih na IT oddelku Ukinitev šolanj administratorjem IT zaradi varčevalne politike vodstva	Varnostni element (požarni zid) lahko postane ozko grlo za internetni prenos podatkov Poraba delovnega časa za posodabljanje in nastavitve Tečaji za IT specialiste so dragi Stalno spremljanje posodobitev proizvajalca in spletnih forumov IT specialistov	Prevzem organizacije s strani konkurenta, ki ima vpeljan standard ISO 27001 Ugodne ponudbe nadaljevalnih tečajev za sistemske administratorje Ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo specialne opreme (outsource) Promocijske cene novih modelov opreme z naprednejšimi možnostmi administracije
3	Strukturni kapital	Posredovanje podatkov interne "Wiki baze" konkurenci Nestimulativna nagrajevalna politika in slaba klima med zaposlenimi v organizaciji Pogosto menjavanje vodstvenega kadra organizacije in spreminjanje prioritet ter strategij Preobremenjenost zaposlenih	Dodatna poraba delovnega časa zaposlenih Podatki strukturiranega znanja (recepture, postopki itd.), ki lahko predstavljajo konkurenč. prednost, lahko z zlorabo pridejo do konkurence Če podatki niso strukturirani po dogovorjenem sistemu in pregledani ter usklajeni z vodji, nimajo posebne vrednosti	Fluktuacija kadra na izpostavljenih mestih v proizvodnji in razvoju programske opreme Široka ponudba programske opreme za strukturirano shranjevanje znanja zaposlenih Prevzem organizacije s strani konkurenta, kjer je dokumentiranje znanja že dobro vpeljano Povezovanje pretoka znanja z inštituti in nevladnimi org.

Priloga 6

Vrstni red	Ime predloga vrzeli	Nevarnosti	Slabosti	Priložnosti
4	Kraja prenosnika, medijev USB itd.	Odtujitev in mogoča zloraba podatkov Otežena prijava policiji po odtujitvi vira (manjkajoča serijska številka) Sprememba pogojev zavarovanja opreme organizacije s strani zavarovalnice Dostop do strateških dokumentov, če gre za prenosnik zaposlenega iz vodstva	Materialna škoda Izguba uporabn. podatkov Možna zloraba podatkov Izgubljeni čas, ko se vzpostavlja novi sistem (ponovne instalacije in vzpostavitev delovnega okolja)	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Ponudba učinkovitih možnosti kriptiranja nosilcev podatkov na trgu Sprememba pogojev zavarovanja prenosne računalniške opreme s strani zavarovalnice Ponudba dodatne zaščite nosilcev podatkov na nivoju hardvera
5	Spremljanje vrzeli na komunikacijski opremi	Instalacija beta popravka (po pomoti) in možni stranski učinki Fluktuacija zaposlenih na IT oddelku Ukinitev šolanj administratorjem IT zaradi varčevalne politike vodstva Neažuriranje dokumentacije nastavitev po zadnjih večjih posegih na konfiguraciji omrežja	Dodatna poraba delovnega časa sistemskega administratorja Stalno spremljanje informacij in opozoril proizvajalca ter spletnih forumov IT special.	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Novi modeli opreme na trgu z zadnjimi verzijami internega programja Ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo specialne opreme (outsource) Ugodne ponudbe nadalj. tečajev za sistemske administratorje
6	Pridobitev uporabniškega imena in gesla	Uporabniško ime in geslo lahko prideta do nepooblaščenih Z zlorabo uporabniškega imena in gesla se na sistemu izvede določeno akcijo, ki ima za organizacijo škodne posledice Dostop do zaupnih dokumentov Nepooblaščen dostop do delovne postaje v času odsotnosti uporabnikov	Kršenje varnostne politike Nepreglednost aktivnih uporabnikov na sistemu (prijava v imenu drugega) Večja ranljivost sistema Dostop do tujega elektronskega predala	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Upoštevanje varnostne politike partnerja s katerim organizacija poslovno sodeluje Zavezujoč pravilnik združenja, v katerem je organizacija Programski vmesniki dostopa do sistema, ki fizično preverjajo uporabnika (prstni odtis)
7	Natisnjeni dokumenti na tiskalniku	Vpogled nepooblaščenih oseb v zaupni dokument Posredovanje podatkov z najdenega izpisa (nezadovoljni zaposleni) konkurenci Odtujitev najdenega izpisa Slabši izhodiščni položaj na pogajanjih, če je prišlo do razkritja vsebine dokumenta konkurenci	Kršenje interne varnostne politike Možnost odtujitve najdenega izpisa Zloraba podatkov izpisa v privatne namene ali škodo organizacije Neprijetnosti v primeru da izpis izgine in iskanje krivca	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Upoštevanje varnostne politike partnerja s katerim organizacija poslovno sodeluje Ponudba tiskalnikov, kjer se uporabnik mora identificirati s službeno kartico, preden natisne dokumet iz tiskalniške vrste Razkritje primera je vzvod za dopolnitev internega pravilnika o varovanju podatkov

Vrstni red	Ime predloga vrzeli	Nevarnosti	Slabosti	Priložnosti
8	Sistemski prostor (sistem zavarovanja)	Samodejni vklop vgrajenega sistema gašenja s prahom (spontano, el. prehodni pojav) Zaostritev pogojev zavarovanja opreme organizacije s strani zavarovalnice Poškodovanje občutljive IT opreme v sistemskem prostoru Gospodarska škoda zaradi nedelujočega sistema	Možne poškodbe na aparaturni opremi Nedelovanje poškodovanih strežnikov v času obnove in servisa Možnost izgube podatkov delovnega dne Nadurno delo zaposlenih v IT oddelku	Prevzem organizacije s strani konkurenta, ki posluje po standardu ISO 27001 Ponudbe zunanjih kvalificiranih ponudnikov za skrbništvo IT (outsource) Upoštevanje varnostne politike partnerja, s katerim organizacija poslovno sodeluje Novi modeli opreme z dodatno varnostno zaščito

Vprašanja za polstrukturirani intervju

1. Ali po vašem mnenju rezultati ocenjevanja dobljenih predlogov kažejo pravo sliko na področju varnosti IS v vaši organizaciji?

2. Kateremu od ocenjenih predlogov bi vi osebno pripisali največjo težo in zakaj?

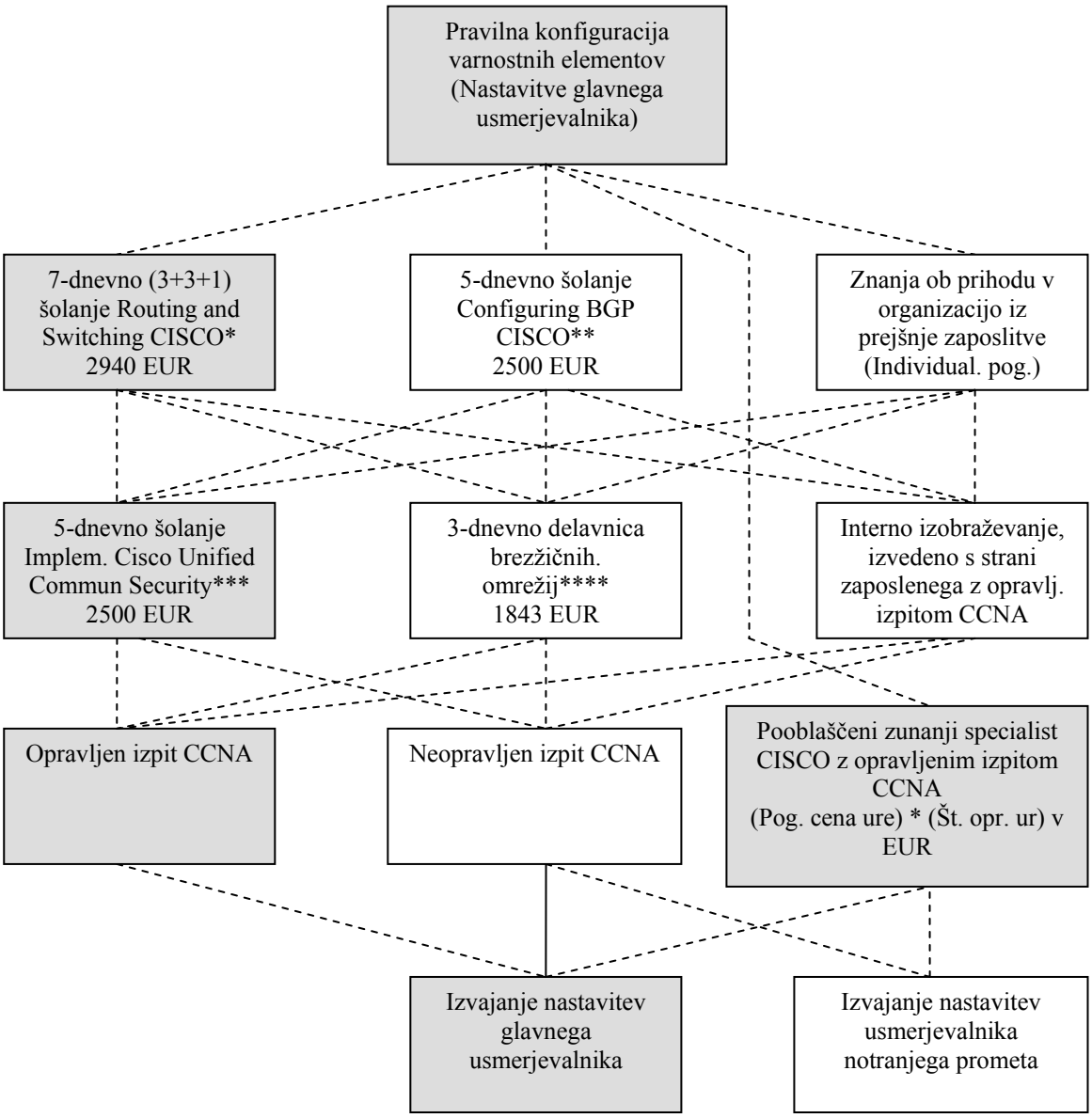
3. Kateri od izbranih predlogov se vam zdi najhitreje izvedljiv? Zakaj?

4. Ali vam bodo dobljeni rezultati ocenjevanja lahko v pomoč pri pripravi nove oz. dopolnjene varnostne politike na področju IS? Za koliko (vaša približna ocena v %) si obetate s tem zmanjšati morebitno tveganje na obravnavanem področju?

5. Ali lahko v grobem ocenite oportunitetni strošek v evrih za najbolje ocenjeni predlog skupine?

6. Kako ocenjujete nov pristop (koncept) za reševanje problematike izboljšanja varnosti IS? Bi z vaše strani morda še kaj dodali?

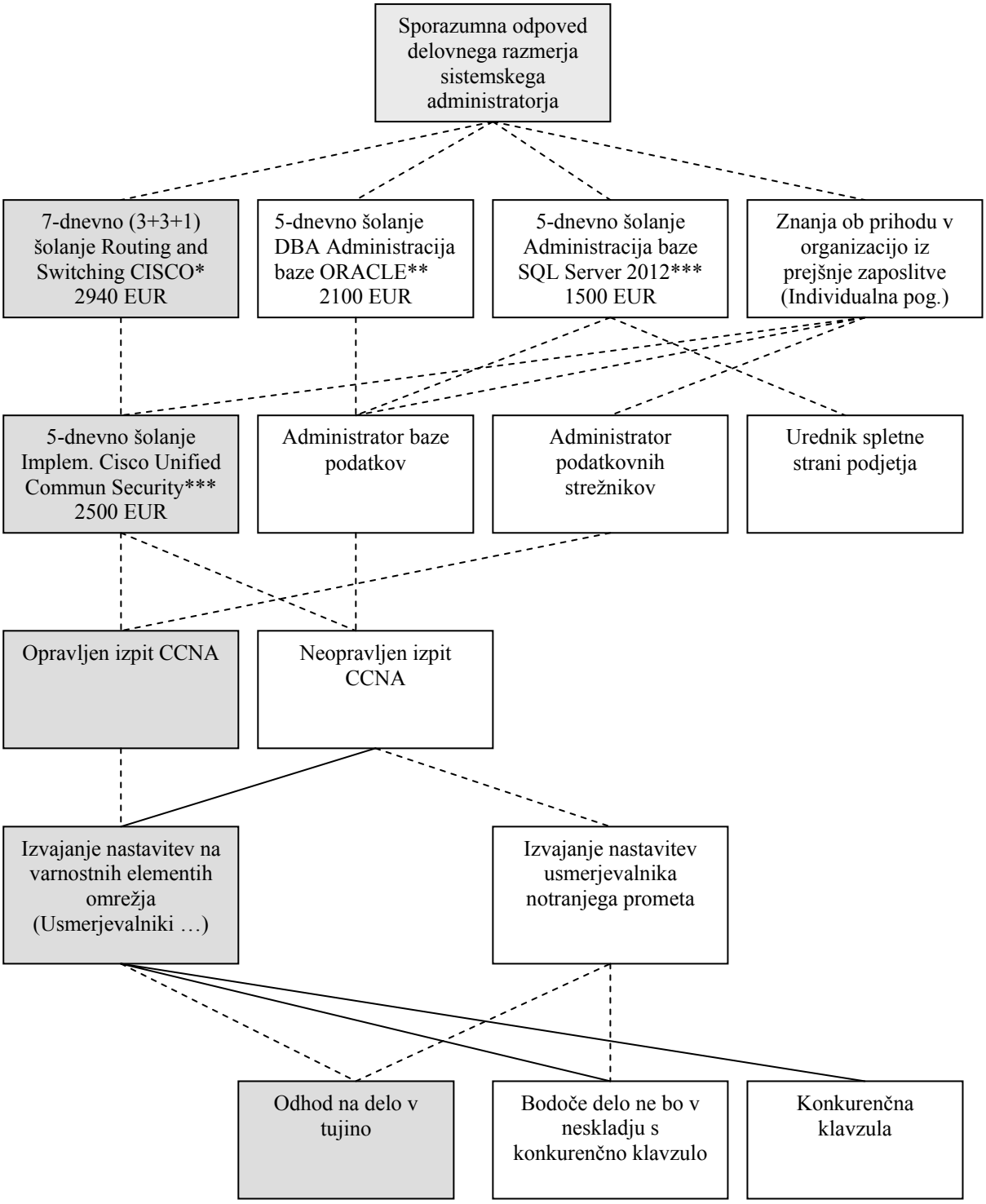
Schneierjev diagram vrzeli IS "pravilna konfiguracija varnostnih elementov omrežja" (2. org.)



* Http://www.avtenta.si/si/izobrazevalni_center/3960/event.html (20. 4. 2012).
** Http://www.avtenta.si/si/izobrazevalni_center/1980/event.html (21. 4. 2012).
*** Http://www.avtenta.si/si/izobrazevalni_center/4258/event.html (21. 4. 2012).
**** Http://www.avtenta.si/si/izobrazevalni_center/4370/event.html (21. 4. 2012).
CCNA – Certified Network Associate.
BGP – Border Gateway Protocol.
Pog. cena ure – cena specialista je pribl. 108 EUR(*).
(*) Http://www.aza-ms.si/cenik.php (21. 4. 2012).
--- Možno; — Ni možno.

Slika 1: Schneierjev diagram vrzeli pravilne konfiguracije varnostnih elementov omrežja

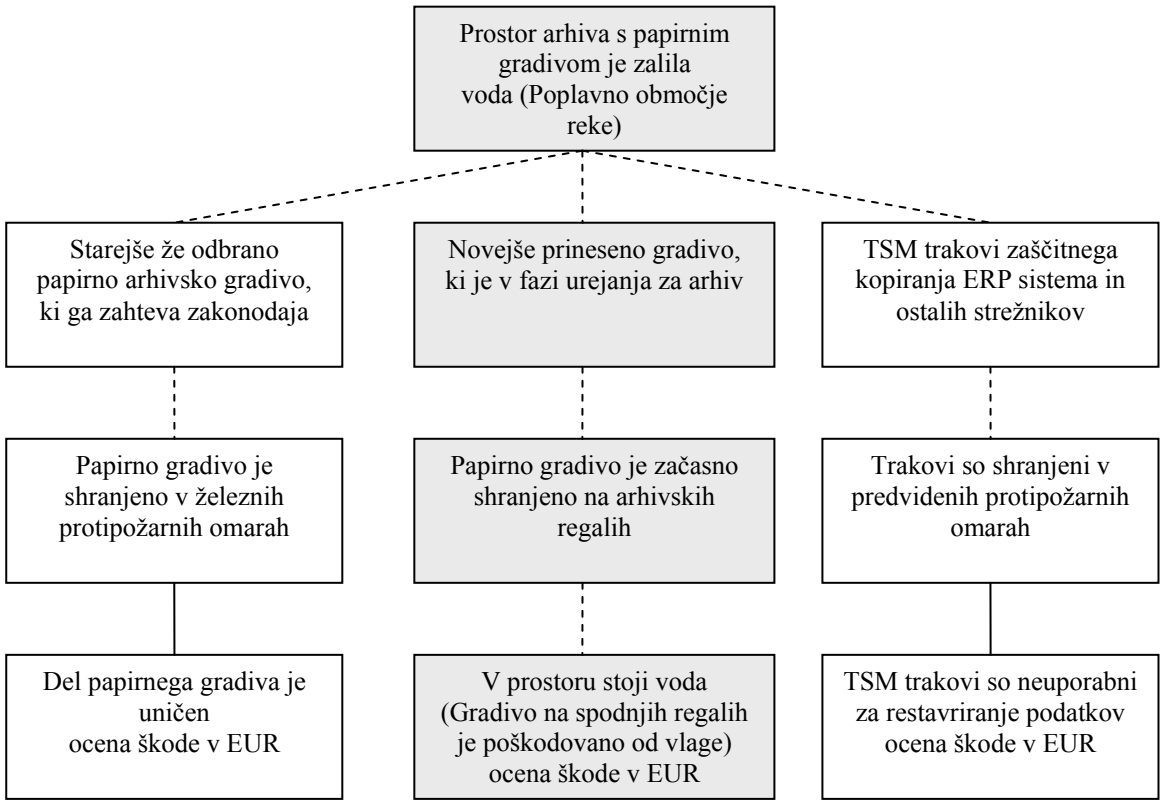
Schneierjev diagram vrzeli IS "strukturni kapital" (2. org.)



* Http://www.avtenta.si/si/izobrazevalni_center/3960/event.html (20. 4. 2012).
** Http://znanje.snt.si/urnik/urnik-oracle-tecaji.shtml (20. 4. 2012).
*** Http://www.kompas-xnet.si/Tecaj/10775A/administering%20sql%20server%202012%20data bases (20. 4. 2012).
DBA – Database Administrator; CCNA – Certified Network Associate.
--- Možno; — Ni možno.

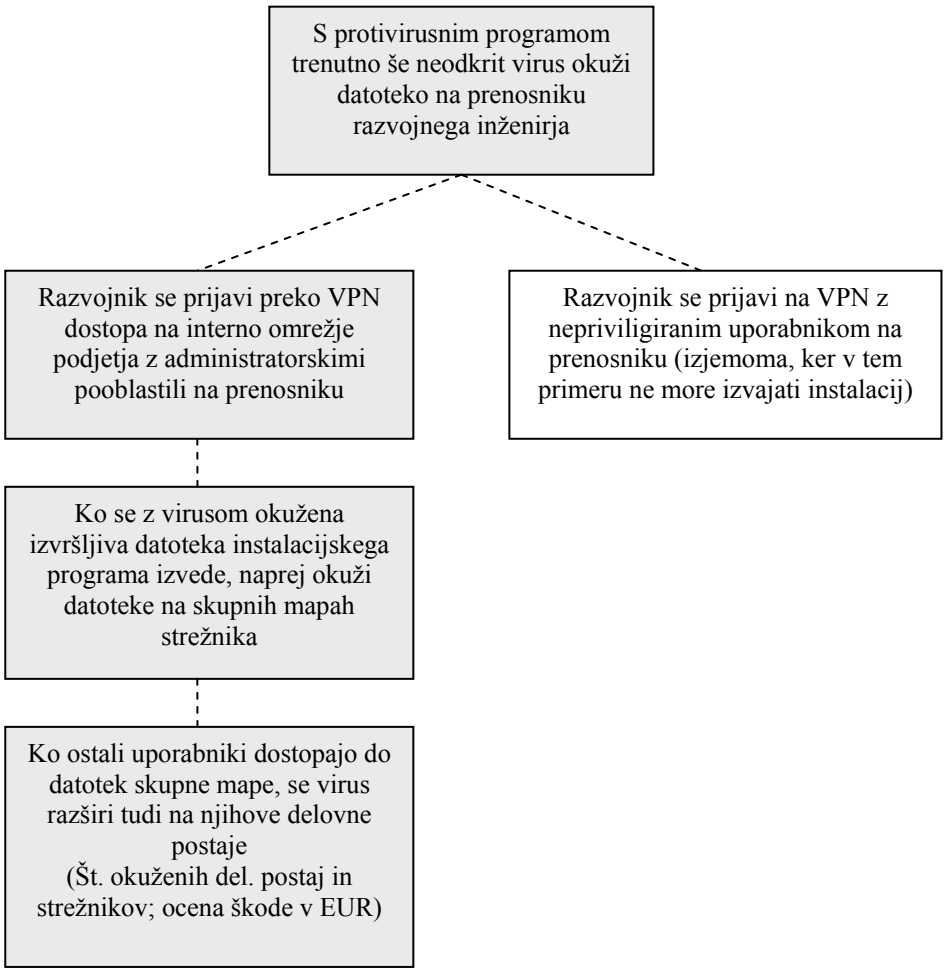
Slika 1: Schneierjev diagram vrzeli strukturnega kapitala

Schneierjev diagram vrzeli IS "neurejen arhiv" (1. org.)



Slika 1: Schneierjev diagram vrzeli neurejenega arhiva

Schneierjev diagram vrzeli IS "VPN dostop do omrežja organizacije" (1. org.)



Slika 1: Schneierjev diagram vrzeli VPN dostopa do omrežja organizacije

Povzetki kategorizacije virov prve organizacije in situacije, kjer se ti pojavljajo v standardu ISO 2005b (v oklepaju sta navedena stran in poglavje omenjenega standarda):

Dokumentacijski podatki,
Elektronska sporočila,
Uporabniška programska oprema,
Prenosni računalniki,
Zaposleni.

DOKUMENTACIJSKI PODATKI

1. ***Ščitenje podatkov in varstvo osebnih podatkov?*** (27002/XIII; 15.1.4)
   - organizacija mora zagotoviti zaščito podatkov in zasebnosti, kot to zahtevajo zadevni zakoni, predpisi, in če je to pomembno, pogodbena določila;
   - organizacija mora razviti politiko za zaščito podatkov in zasebnosti. S to politiko je treba seznaniti vse osebe, ki sodelujejo pri obdelavi osebnih podatkov.

2. ***Zaščita organizacijskih zapisov?*** (27002/XIII; 15.1.3)(258)
   - Pomembne zapise je treba zaščititi pred izgubo, uničenjem ali potvarjanjem; zaščita naj bo v skladu z zahtevami, ki jih določajo statuti, predpisi, pogodbe in v skladu s poslovnimi zahtevami;
   - zapise je treba kategorizirati, npr. računovodski zapisi, zapisi podatkovnih baz, zapisi poslovanja, presojni zapisi in operacijski postopki;
   - nosilci podatkov, ki se uporabljajo za shranjevanje zapisov, se lahko s časom poškodujejo. Postopke shranjevanja in ravnanja s temi nosilci je zato treba vpeljati v skladu s priporočili proizvajalca.

3. ***So pri določanju klasifikacijskih ravni dokumenti s podobnimi varnostnimi zahtevami obravnavani skupaj?*** (Ali lahko to pripomore k poenostavitvi klasifikacije?) (27002/27)

4. ***So naslovniki in telefonski imeniki, ki kažejo, kje se nahajajo zmogljivosti za obdelavo občutljivih informacij, neposredno dostopni javnosti?*** (27002/39; 9.1.3)

5. ***Kako se ravna z zaupnimi izpisi?*** (27002/47; 10.1.1 (f); 10.7.2, 10.7.3)
   - Kadar se nosilci podatkov ne potrebujejo več, jih je treba zanesljivo in varno odstraniti z uporabo uradnih postopkov;
   - postopki za varno odstranitev nosilcev z občutljivimi podatki morajo biti usklajeni z občutljivostjo teh informacij;
   - kjer je to mogoče, je treba odstranitve občutljivih predmetov beležiti, da se ohrani presojna sled.

ELEKTRONSKA SPOROČILA

1. ***Ali se službeno el. pošto usmerja v oblak (gmail, yahoo, hotmail, …)?***

2. ***So določena pravila za uporabo el. pošte in interneta?*** (27002/26)
   - Postopki in kontrole, ki jih je treba upoštevati, naj bi vključevali:
     a) postopke za zaščito sporočenih občutljivih elektronskih informacij v obliki priponk;
     b) postopke za odkrivanje in zaščito pred zlonamerno kodo;
     c) uporabo kriptografskih tehnik, npr. za zaščito zaupnosti, celovitosti in verodostojnosti informacij.

3. ***So uporabniki seznanjeni s problemom potegavščin in znajo ravnati v primeru prejema le-te?*** (27002/52)
   - vpeljevanje postopkov za preverjanje informacij v zvezi z zlonamerno kodo in zagotovitev, da so opozorilni letaki pravilni in informativni;
   - vodje morajo zagotoviti, da se za razlikovanje med potegavščinami in pravimi zlonamernimi kodami uporabljajo kvalificirani viri (ugledni časopisi, zanesljive internetne strani);
   - vsi uporabniki morajo biti seznanjeni s problemom potegavščin ter morajo vedeti, kako ravnati v primeru prejema le-te.

4. ***Kontrole glede samodejnega pošiljanja elektronske pošte?*** (27002/62)
   - kontrole in omejitve glede samodejnega posredovanja elektronske pošte na zunanje poštne naslove.

5. ***Vključen asistent odsotnosti?*** (nadomeščanje)

UPORABNIŠKA PROGRAMSKA OPREMA

1. ***Je prišlo do zastoja poslovanja zaradi zlonamerne kode?*** (27002/pogl.10.4)
   - Potrebno je uvesti varnostne ukrepe, da se prepreči in odkrije vnos zlonamerne kode in nepooblaščene prenosne kode;
   - treba je vpeljati kontrole za preprečevanje, odkrivanje in odpravo te kode, obenem pa je treba vpeljati ustrezne postopke za ozaveščanje uporabnikov;
   - izvajanje rednih pregledov programske opreme in podatkov na sistemih, ki podpirajo pomembne poslovne procese; prisotnost kakršnih koli neodobrenih datotek ali nepooblaščenih dodatkov je treba uradno raziskati;
   - preverjanje prisotnosti zlonamerne kode v vseh priponkah elektronske pošte in naloženih datotekah pred uporabo;
   - preverjanje, ali spletne strani vsebujejo zlonamerno kodo.

2. ***So določene odgovornosti povezane z namestitvijo in vzdrževanjem programske opreme?*** (27002/21)
   - Sporazumi s tretjimi strankami, ki vključujejo upravljanje z zmogljivostmi za obdelavo informacij organizacije ali dodajanje izdelkov ali storitev zmogljivostim za obdelavo informacij, morajo vsebovati vse pomembne varnostne zahteve;
   - odgovornosti, povezane z namestitvijo in vzdrževanjem strojne in programske opreme.

3. ***So pripravljeni načrti za neprekinjeno poslovanje po napadih zlonamerne kode?*** (27002/52)
   - Se redno posodablja programska oprema za odkrivanje in odpravljanje zlonamerne kode? (27002/52)
   - Se uporablja eden ali dva programska izdelka za zaščito pred zlonamerno kodo? (27002/52)

4. ***So določena in dokumentirana pravila za prehod programske opreme iz razvojne v produkcijsko fazo?*** (27002/49; 10.1.4)
   - Razvojne, testne in produkcijske zmogljivosti je treba ločevati, da se zmanjša nevarnost nepooblaščenega dostopa ali spremembe produkcijskega sistema;
   - treba je določiti stopnjo ločenosti med produkcijskim, testnim in razvojnim okoljem, ki je potrebna za preprečitev produkcijskih težav, ter vpeljati ustrezne kontrole;

- tudi osebje, ki se ukvarja z razvojem in testiranjem, predstavlja nevarnost za zaupnost produkcijskih informacij;
- razvoj in testiranje lahko povzročita resne težave, npr. nezaželeno spremembo datotek ali sistemskega okolja ali sistemsko okvaro.

PRENOSNI RAČUNALNIKI

1. ***Osebne zmogljivosti (prenosni računalniki, domači računalniki in ročne naprave za obdelavo poslovnih informacij; vir novih ranljivosti)?*** (27002/14; 6.1.4)
   - Treba je opredeliti in vpeljati postopek, s katerim vodstvo odobri takšne zmogljivosti za obdelavo informacij;
   - treba je prepoznati in vpeljati potrebne kontrole.

2. ***Ali ima organizacija uradno politiko in ustrezne varnostne ukrepe za zaščito pred tveganji, ki jih prinaša uporaba prenosnih računalnikov in prenosnih računalniških zmogljivosti?*** (27002/94; 11.7.1)
   - Pri uporabi prenosnih računalniških in komunikacijskih zmogljivosti, kot so notesniki, dlančniki, prenosni računalniki, pametne kartice in mobilni telefoni, je treba posebej paziti, da se ne ogrozi varnost poslovnih informacij;
   - politika za delo s prenosnimi računalniki mora vključevati zahteve po fizični zaščiti, nadzorovanju dostopa, kriptografskih tehnikah, varnostnih kopijah in po protivirusni zaščiti;
   - prenosne računalniške naprave naj bodo tudi fizično zaščitene pred krajo, zlasti kadar jih na primer pustimo v avtomobilu ali v drugem prevoznem sredstvu, v hotelski sobi, v konferenčnih centrih ali v prostorih, kjer se srečujejo ljudje.

3. ***So določene smernice za uporabo prenosnih naprav, še posebej, ko se te uporabljajo zunaj prostorov organizacije?*** (27002/26; 7.1.3;11.7.1)
   - Vsi zaposleni, pogodbeniki in uporabniki tretje stranke morajo upoštevati pravila za sprejemljivo uporabo informacij in virov;
   - zadevno vodstvo mora zagotoviti posebna pravila ali navodila;
   - zaposleni, pogodbeniki in uporabniki tretje stranke, ki uporabljajo ali imajo dostop do virov organizacije, morajo poznati obstoječe meje, ki veljajo za njihovo uporabo informacij in virov organizacije.

4. ***So dokumentirani postopki kot zagon in zaustavitev računalnika, vzdrževanje opreme, ravnanje z nosilci podatkov, upravljanje računalniških sob in ravnanje s pošto ter varovanje?*** (27002/47; 10.1.1)
   - V delovnih postopkih morajo biti podrobno navedena navodila za natančno izvajanje vsakega dela;
   a) z iskanjem pomoči v primeru nepričakovanih produkcijskih ali tehničnih težav;
   b) s postopki za ponovni zagon in reševanje sistema po zastoju;
   c) za upravljanje s presojnimi sledmi in informacijami iz dnevnika o delovanju sistema.

ZAPOSLENI

1. ***Varstvo osebnih podatkov?***

2. ***Kako je dodeljena odgovornost pri varovanju informacij?***

3. ***Se ozavešča, izobražuje in usposablja za varovanje informacij?***

4. ***So vpeljana merila, ki se uporabljajo za ocenjevanje kakovosti upravljanja, varovanja informacij in odziv uporabnikov s predlogi za izboljšavo?***

5. ***Je urejeno nadomeščanje, tako da posamezniki z dodeljenimi odgovornostmi pri varovanju svoje naloge zaupajo drugim?*** (27002/12;6.1.3)
   - Vse odgovornosti pri varovanju informacij morajo biti natančno določene;
   - treba je jasno določiti odgovornosti za zaščito posameznih virov ter za izpeljavo posebnih varnostnih postopkov;
   - treba je imenovati osebo, ki je odgovorna za vsak vir ali varnostni postopek, ter dokumentirati podrobnosti v zvezi z njegovimi odgovornostmi.

6. ***Je določen lastnik posameznega vira, ki prevzema odgovornost za njegovo vsakodnevno zaščito?*** (27002/13;6.1.3)
   - Pogosto se imenuje lastnik vsakega vira, ki nato prevzame odgovornost za njegovo vsakodnevno zaščito.
   a. ***Obstaja oseba, ki je odgovorna za vzdrževanje ustreznih kontrol?*** (27002/24)
   b. ***So viri jasno prepoznani?***
   c. ***Obstaja seznam vseh pomembnih virov?*** (27002/24)
      (Postopek popisovanja virov je pomemben predpogoj za upravljanje tveganja)
   d. ***So prepoznani in dokumentirani vsi pomembni viri?***

Polstrukturirani intervju (1. org.)

Za vodilo srečanja smo pripravili šest vprašanj, ki so v prilogi 7. Soočili smo poglede na odkrite nevarnosti IS organizacije in predlagane rešitve zanje. Zastavljena vprašanja in odgovori nanje so v nadaljevanju:

1. Ali po vašem mnenju rezultati ocenjevanja dobljenih predlogov kažejo pravo sliko na področju varnosti IS v vaši organizaciji?

Vodja IT: Dobljeni predlogi s strani zaposlenih večinoma odsevajo pravo sliko glede varnosti IS. Kažejo na probleme, ki jih vodstvo IT pozna in se jih zaveda. Na nekaterih področjih so bile že nedavno sprožene aktivnosti za izboljšanje situacije in zmanjšanje tveganja, pripravljamo pa tudi nov dokument varnostne politike s področja informacijske varnosti, ki naj bi nadomestil predhodni predpis o informacijski varnosti v organizaciji. Intenzivno se dela na rezervni lokaciji v bližini organizacije, ki je že izven poplavno ogroženega dela in leži nad strugo reke. Na rezervno lokacijo se bo po interni LAN povezavi s pasovno širino 1GB dnevno kopiralo popolne podatke ključnih dveh baz (baze ERP sistema in baze programske rešitve, kjer se hrani elektronska pošta, dokumentacija v elektronski obliki in podatki številnih manjših uporabniških programov). S tem bi bilo omogočeno restavriranje podatkov zadnjega delovnega dne. Doslej se kasete zaščitnega kopiranja hranijo v sistemskem prostoru, mesečno pa se iznašajo v zaščiteno železno omaro v eno od stavb na lokaciji.

2. Kateremu od ocenjenih predlogov bi vi osebno pripisali največjo težo in zakaj?

Vodja IT: Dosegljivosti ERP sistema in stanju arhivskih podatkov. Pri tem mislim tako elektronske podatke na trakovih kot papirne, ki jih moramo hraniti že zaradi zakonodaje. Število licenc ERP sistema je omejeno in povezano s precejšnjimi stroški. Eno licenco trenutno uporablja več uporabnikov, saj je delo v organizaciji organizirano v dopoldanski in popoldanski izmeni. Na to licenco so določene avtorizacije za posamezne module programske rešitve, ki jih potrebujejo vsi. To z vidika varnosti pomeni nekoliko večje tveganje. Varnostnih incidentov doslej ni bilo. Število licenc bomo zaradi zmanjšanja tveganja v prihodnjem obdobju dvignili za 20 %.

Drugi predlog je arhiviranje podatkov IS. Gradi se na objektu na ločeni lokaciji v bližini organizacije. Tja naj bi se dnevno kopiralo ključne podatke ERP sistema, elektronske pošte in ostalih specializiranih programskih rešitev za delo v razvoju, nabavi in prodaji (obdelave reklamacij, kartotek orodij, postopki vzdrževanja itd.). V sklop kopiranja sodijo tudi podatki, shranjeni na datotečnih strežnikih platform Unix in Linux.

3. Kateri od izbranih predlogov se vam zdi najhitreje izvedljiv? Zakaj?

Vodja IT: Predlog, povezan s standardnimi in lahko uganljivimi gesli. Rešitev je mogoča v tednu dni. Že doslej je veljal na področju IS organizacijski predpis, da se gesla za prijavo na delovne postaje in strežnike periodično menjajo. Uporabniki, ki ta interes imajo, temu tudi redno sledijo. Potrebna pa bo dodatna kontrola izvajanja tega ukrepa.

4. Ali vam bodo dobljeni rezultati ocenjevanja lahko v pomoč pri pripravi nove oz. dopolnjene varnostne politike na področju IS? Za koliko (vaša približna ocena v %) si obetate s tem zmanjšanje morebitnega tveganja na obravnavanem področju?

Vodja IT: Dobljene rezultate bomo upoštevali pri pisanju nove varnostne politike IS za organizacijo. Doslej je veljalo, da se je s to problematiko ukvarjal le ožji krog zaposlenih na oddelku informatike. V tem primeru pa gre za pozitivno izkušnjo, ker je na določeno problematiko opozoril tudi krog izbranih zaposlenih tako prve kot druge skupine. Težko je sicer v tem trenutku dati oceno v odstotkih, obetamo pa si izboljšanje informacijske varnosti za okoli 20 %.

5. Ali lahko v grobem ocenite oportunitetni strošek v evrih za najbolje ocenjeni predlog skupine?

Vodja IT: Za oceno oportunitetnega stroška najbolje ocenjenega predloga je brez podrobno opravljene analize posamezne grožnje težko dati oceno. Vse je zelo odvisno od okoliščin in od primera do primera. Gleda na to da je organizacija OEM partner svetovno znanim koncernom, lahko z uhajanjem informacij iz organizacije nastane škoda velikosti 10.000 do nekaj 100.000 EUR. Organizacija namreč izpelje razvoj in izdelavo posameznih sklopov za omenjene stranke. Varovanje teh informacij je zato zelo velikega pomena, saj se ti izdelki naprej prodajajo pod svetovno znanimi blagovnimi znamkami.

6. Kako ocenjujete nov pristop (koncept) za reševanje problematike izboljšanja varnosti IS? Bi z vaše strani morda še kaj dodali?

Vodja IT: Nov pristop reševanja problematike je dobrodošel, ker so vanj vključeni tudi ostali zaposleni. Že samo s tem, ko aktivno sodelujejo, se dvigne njihova ozaveščenost za vsa ta vprašanja, s svojo izkušnjo pa bodo lahko vplivali tudi na ostale zaposlene.

Polstrukturirani intervju (2. org.)

Obravnavali smo odkrite nevarnosti IS v organizaciji in predlagane rešitve zanje. Identiteta ostalih dveh sogovornikov, ki sta bila razen direktorja prisotna na intervjuju, je pojasnjena v fazi 1. Vprašanja in odgovori sodelujočih so v nadaljevanju:

1. Ali po vašem mnenju rezultati ocenjevanj dobljenih predlogov kažejo pravo sliko na področju varnosti IS v vaši organizaciji?

Direktor: Zaposleni so povedali svoje videnje stanja problema. Rezultati to stanje tudi kažejo, če gre za normalno in odgovorno fizično zaščito podatkov. Dobro je, da smo dobili možne ranljivosti, o katerih se je skozi pogovor z zaposlenimi iz vseh delov organizacije razmišljalo. Dobljeni predlogi lahko predstavljajo križišče za naslednjih deset novih, ki so morda zanemarljivi z dobljenimi, ponovno pa se lahko pregleda, kaj je mogoče izboljšati. Rezultati so lahko iztočnica za pripravo nove ocene tveganja.

Beseda je tekla o pametnem telefonu, ki je bil kot predlog spoznan za največjo nevarnost IS.

Direktor: Pametni telefon je ena izmed dodatnih in težje nadzorljivih vstopnih točk v IS organizacije. Pod nadzorom so sicer vsi ostali načini dostopa (npr. internet). Zavedamo se namreč, da v organizaciji hranimo in imamo dostop do številnih osebnih podatkov drugih. Teoretično obstaja možnost, da bi preko te naprave z grožnjo nad zaposlenim lahko prišlo do zlorabe omenjenih podatkov.

Oseba B: Kdorkoli od zaposlenih lahko pride do podatkov, če to res hoče, odvisno pa je od tega, koliko je sposoben te podatke zlorabiti in oplemenititi. Zavedamo se, da zadostuje že en sam tak primer, ki širi slab glas o organizaciji.

2. Kateremu od ocenjenih predlogov bi vi osebno pripisali največjo težo in zakaj?

Direktor/oseba A/oseba B: Pametnemu telefonu.
Poleg prvega predloga pa še:
Oseba B: Strukturnemu kapitalu.
Oseba A: Kraji prenosnika in medijev USB.

Enotni so si bili tudi glede pomena drugouvrščenega predloga (pravilna konfiguracija varnostnih elementov). Ta namreč rešuje marsikatero kasnejšo zagato na področju varnosti podatkov v elektronski obliki kot tudi dostopnosti pametnih telefonov v interno komunikacijsko omrežje. Dodamo lahko še, da obravnavani informacijsko vir že dolgo ni več le telefon za telefoniranje in pošiljanje sporočil. Njegovo jedro tvori pravi operacijski sistem,

ki omogoča zagon številnih uporabnih programskih rešitev (elektronsko pošto, branje PDF dokumentov, koledar z beležnico in opomnikom, dostop do interneta, navigacijo in še številne druge).

3. Kateri od izbranih predlogov se vam zdi najhitreje izvedljiv? Zakaj?

Direktor/oseba A/oseba B: Predlog konfiguracije varnostnih elementov.
Direktor: S tem se namreč omeji "vhodna vrata". Če je to pravilno in po dogovoru nastavljeno, je vseh drugih problemov veliko manj.

Na srečanju smo omenili tudi interni pravilnik, po katerem se Facebook ne sme uporabljati v organizaciji. Tako omejitev lahko učinkovito reši že ena od nastavitev usmerjevalnika, ki sodi med te varnostne elemente.

4. Ali vam bodo dobljeni rezultati ocenjevanja lahko v pomoč pri pripravi nove oz. dopolnjene varnostne politike na področju IS? Za koliko (vaša približna ocena v %) si s tem obetate zmanjšanje morebitnega tveganja na obravnavanem področju?

Direktor: Dobljeni rezultati potrjujejo, kaj je bilo doslej storjenega glede na prejšnjo oceno tveganja in omogočajo predvidevanje planov za naprej. Ocena tveganja mora biti v skladu s certifikatom ISO 27001:2005 napravljena po isti metodologiji, tako da je mogoče ob koncu primerjati rezultate. V primerjavi s preteklim letom je bil na področju varnosti podatkov dosežen velik napredek in smo lahko z doseženim zadovoljni. Med zaposlenimi smo usposobili tudi svoje presojevalce za področje varovanja podatkov in informacij. O približni oceni zmanjšanja tveganja v odstotkih se žal niso znali jasneje opredeliti.

5. Ali lahko v grobem ocenite oportunitetni strošek v evrih za najbolje ocenjeni predlog skupine?

Direktor: Na to je zelo težko odgovoriti. Okolje je dinamično in razmerja posameznih kategorij, ki so v igri določenega incidenta ali morebitne grožnje, se neprestano spreminjajo. Če se nekaj ne zgodi, se niti ne zavedamo, kaj vse bi to utegnilo potegniti za sabo. Tudi če se nekaj zgodi, se v prvem hipu ne ve, kakšen je strošek in celotna škoda.

Oseba C: Že to, da zaposleni vedo, da se v organizaciji gradi sistem vodenja varovanja informacij, je lahko za marsikoga dovolj, da se v določena tveganja na teh področjih sploh ne spušča. Ljudje vidijo, da se na tem resno dela, da je vzpostavljen določen sistem varovanja in da je stvar pod nadzorom.

Direktor: Marsikaj je mogoče in če nekaj zaposleni povzroči, se ga tudi najde. Na zunaj smo zaščiteni s tehniko, kolikor ta to omogoča. K temu nedvomno sodijo še zaposleni, ki naj bi z gesli varovali to, kar so dolžni. V organizaciji smo nedavno posebej za namen nadaljnjega organiziranja aktivnosti varovanja informacij zaposlili strokovnjaka, ki ima na področju varnosti veliko izkušenj in opravljene številne certifikate ter za to vse potrebne kompetence. Na operativnem nivoju sodi zraven tudi oseba B.

6. Kako ocenjujete nov pristop (koncept) za reševanje problematike izboljšanja varnosti IS? Bi z vaše strani morda še kaj dodali?

Direktor: Gre za preizkus ene od metod, ki dodatno vključuje zaposlene in ki omogoča, da se z drugega zornega kota pogleda, kaj je bilo storjenega na področju varovanja informacij in kje potencialne ranljivosti sistema še obstajajo. Konceptu pripisujem prednost prav v razpršenosti in vključitvi zaposlenih iz celotne organizacije. Naloga osebe B bo, da skrbno prouči dobljene rezultate in skuša v preseku s svojim tehničnim poznavanjem problematike napraviti najprej oceno trenutne zaščite dobljenih ranljivosti. Nato bo sledila določitev prioritet in nadaljnje reševanje posameznih področij.

Oseba C: Zaposleni, ki so sodelovali na prvem in drugem srečanju, bodo svojo izkušnjo lahko širili naprej tudi na ostale zaposlene.

Po obisku v organizaciji lahko dodamo, da verjetno brez direktorjevega pragmatičnega pogleda na varnost informacij, organizacijskega talenta in odobritve vseh aktivnosti organizacija ne bi bila na področju varovanja informacij tako daleč, kot je.