Univerza v Mariboru

Fakulteta za organizacijske vede

Magistrsko delo
Management informacijskih sistemov
Analiza in načrtovanje informacijskih sistemov

ČLOVEŠKI VIDIK VARNOSTI RAČUNALNIŠTVA V OBLAKU

Mentor: red. prof. dr. Robert Leskovar

Kandidatka: Nataša Maraž

Kranj, september 2016

ZAHVALA

Zahvaljujem se mentorju red. prof. dr. Robertu Leskovarju za pomoč in strokovno vodenje pri opravljanju magistrskega dela.

Zahvala gre tudi dr. Nataši Demšar Pečak za prispevek k nastajanju te naloge in mag. Liljani Djakić za lektoriranje.

Posebna zahvala velja mojim staršem, možu in sinovoma, ker so me ves čas študija spodbujali in verjeli v enega izmed mojih zastavljenih ciljev.

POVZETEK

Magistrska naloga obravnava človeške aspekte varnosti računalništva v oblaku. Predstavljen je pregled literature na področju oblačnih storitev oziroma računalništva v oblaku. Podan je tudi pregled uporabe oblačnih storitev z vidika posameznika in organizacij, še posebej pri storitvah v bančništvu. Zaradi čedalje večje uporabe oblačnih storitev v bančništvu je opredeljen pristop ohranjanja informacijske varnosti, ki jih zagotavljajo tri glavne dimenzije. Navedene so tudi trenutno veljavne regulatorne zahteve in priporočila politike uporabe zunanjih izvajalcev, kot tudi veljavna zakonodaja na področju varovanja podatkov. Podrobneje je opisan psihološki vidik varnosti v virtualnem prostoru, saj je varovanje informacij pred osebjem in zunanjimi izvajalci zelo pomembno področje varovanja informacij. Notranje osebje, torej zaposleni, predstavljajo največje tveganje in lahko povzročijo največ škode, kljub temu pa se najpogosteje zanemarjajo kot varnostna grožnja. Poudarjeni so socialni inženiring, oblike samopomoči in opolnomočenje. Kot pomemben element varovanja podatkov je izpostavljen pomen zaupanja tako v operacijski sistem in strojno oz. tehnično opremo, kot tudi v osebje oziroma zaposlene v organizaciji. Analiziranih in opisanih je nekaj odmevnih primerov delovanja posameznikov in skupin, ki so povzročile varnostne incidente oz. zlorab oblačnih storitev in njihove posledice. Naveden je primer dobre prakse usposabljanja zaposlenih za varno uporabo oblačnih storitev v javni upravi z veljavno zakonodajo in možnimi rešitvami. V grafičnem prikazu je predstavljen model usposabljanja zaposlenih za varno uporabo oblačnih storitev, ki temelji na upoštevanju kombinacije usposobljenega osebja, postopkov in tehnologije ter navodil oziroma informacij s katerimi se lahko zagotovi varnost. Model vključuje tudi sistem SUVI, ki je natančneje opredeljen. Kot pomemben povezovalni element modela usposabljanja nastopa ozaveščenost o varnosti oziroma varni uporabi oblačnih storitev. V ekranskih slikah in z vsebinsko razlago je predstavljen poenostavljen primer usposabljanja zaposlenih za varno uporabo oblačnih storitev.

KLJUČNE BESEDE:

- računalništvo v oblaku,
- kibernetska varnost,
- zloraba informacij,
- ozaveščenost,
- oblačne storitve v bančništvu,
- model izobraževanja in usposabljanja zaposlenih za varno uporabo oblačnih storitev

ABSTRACT

This Master's thesis deals with the human aspect of cloud computing security. It provides an overview of the literature available in the field of cloud services or cloud computing and an overview of the use of cloud services from the perspective of individuals and organisations, particularly for those services used in banking. The growing use of cloud computing in banking requires a new approach to information security management, which is presented within three main dimensions. It also lists the currently applicable regulatory requirements and outsourcing policy recommendations, as well as the applicable legislation in the field of data protection. It describes in detail the psychological aspects of cyber security, since the protection of information against staff and external service providers is an extremely important element in information security.

Internal staff or employees represent the greatest risk and can cause most damage, however they often seem to be ignored as a security threat. The main highlights in this respect are social engineering, self-help and empowerment. An important data protection element is trust in the operating and hardware systems as well as the staff or employees working in the organisation. Several high-profile security breaches conducted by individuals or groups and their implications have been analysed and presented, as they led either to security incidents or abuse of information. There is also a good practice case of employee training on safe use of cloud services by the public administration with the applicable legislation and potential solutions.

The graphic presentation shows a model of education and training of employees for safe use of cloud services based on the combination of employees' skills, procedures and technology as well as security instructions or information. The model also consists of the Information Security Management System (ISMS), which is presented in detail. Raising the awareness of safety or safe use of cloud services is an important binding element in the training model. A simplified employee training model on safe use of cloud services is therefore provided along with the screen prints and text describing the activities.

KEYWORDS:

- cloud computing,
- cyber security,
- abuse of information,
- awareness,
- cloud computing in banking,
- model of education and training of employees for safe use of cloud services

KAZALO

1. UVOD

Računalništvo v oblaku oziroma oblačne storitve so v zadnjih letih zavzele pomembno mesto v vsakodnevnem življenju posameznikov in organizacij. Tako zasebno kot tudi poslovno omogočajo dostop do digitalnih podatkov, ne glede na to, kdaj in od kod se do njih dostopa. S tem je omogočen takojšnji dostop do omrežja, pomnilniških enot, strojne opreme, programske opreme, različnih informacijskih storitev, itd.

Kljub velikemu povpraševanju je uporaba nove tehnologije še vedno relativno nizka, razlogi za trenutne razmere pa so predvsem v slabi ozaveščenosti širše javnosti in oteženem nadzoru nad digitalnim okoljem, torej posledično vprašanju varnosti lastnine, ki jo objavimo/shranimo v virtualnem okolju. Zlorabe, povezane z oblačnimi storitvami, povzročajo veliko materialno pa tudi nematerialno škodo posameznikom in organizacijam, kljub temu pa so z vidika človeških aspektov varnosti manj natančno preučene. Organizacijski vidiki obnašanja tako zaposlenih kot povzročiteljev nevarnosti so sorazmerno dobro raziskani v klasični literaturi. Modeli usposabljanja in zgodnjega odkrivanja nevarnega obnašanja zaposlenih so redki, zaviti v tančico skrivnosti, implementacija pa zelo draga. Gre za sisteme, kjer obstoječe kontrole človeškega aspekta ne zaznajo ali ne morejo zaznati visokega tveganja, čigar posledica so lahko izguba premoženja, ugleda, dostojanstva ali celo življenja.

Prav zato pa so postali podatki, tako poslovni kot zasebni, ranljivi, saj so v trenutku dostopni vsem, tudi nepooblaščenim uporabnikom. Zato je zelo pomembno, da uporabniki upoštevajo določena pravila in s tem zmanjšujejo tveganje za materialno ali nematerialno škodo (zloraba osebnih podatkov, zloraba identitete), krajo denarja, včasih celo izgubo življenja.

Kadar pride do vdora v sistem organizacije, na primer banke, lahko to negativno vpliva na podobo organizacije in zaupanje tako obstoječih kot potencialnih strank. Hőllwarth (2012) navaja, da mora imeti banka, ki iznaša podatke, stalen nadzor nad svojo osrednjo dejavnostjo. V zvezi z računalništvom v oblaku je zelo pomembno, da hrambo podatkov vedno razumemo kot iznos/zunanje izvajanje. Prav zato pa je tako pomembna uporaba strogih načel in upoštevanje pravil informacijske varnosti.

2. METODOLOGIJA DELA

2.1. PREDSTAVITEV PROBLEMA

Oblačne storitve oz. računalništvo v oblaku, ki se pogosto uporablja kot metafora za internet, so v zadnjih letih zavzele pomembno mesto v vsakodnevnem življenju posameznikov in organizacij (Jurič, Frece, Hertiš & Srdič, 2009, str. 2). Tehnologijo podatkovnega oblaka opredeljujemo kot vejo informacijske tehnologije, ki s svojim razvojem pomembno vpliva na temeljne spremembe računalniških sistemov.

Uporabniku za uporabo programov ali določenih strojnih karakteristik ni več potreben nakup izdelkov, ampak lahko potrebne elemente enostavno zakupi oziroma najame preko spleta. Računalništvo v oblaku omogoča takojšnji dostop do omrežja, strojne opreme, pomnilniških enot, programske opreme, različnih informacijskih storitev, torej do prednastavljenih skupnih informacijskih virov, ki so lahko uporabniku na razpolago praktično takoj. Oblačne storitve oblikuje 5 bistvenih značilnosti, 3 storitveni modeli in 4 izvedbeni modeli, o katerih bomo govorili kasneje.

Uporaba interneta nam sicer olajša komunikacijo z drugimi, ne glede na zemljepisne oddaljenosti, smo pa zato na omrežju toliko bolj izpostavljeni različnim varnostnim tveganjem. Z izkoriščanjem varnostnih lukenj, ranljivosti v programski opremi in tudi v naših vedenjskih vzorcih, lahko tujci pridobijo nadzor nad našo opremo, podatki in nenazadnje tudi denarjem (Mešič, 2011, 11).

Največja skrb računalništva v oblaku je varnost, kar je potrdila tudi raziskava Harvard Business Review, saj je preko 50% uporabnikov izrazilo zaskrbljenost zaradi varnostni podatkov (Knorr & Gallen, 2011). Celovit pristop k ohranjanju informacijske varnosti zagotavljajo številne razsežnosti, tri glavne dimenzije pa so (Meier, 2003):

- *zaupnost (ang. confidentiality)*: zaščita informacij pred nepooblaščenim razkritjem,
- *celovitost (ang. integrity)*: zaščita informacij pred nepooblaščenimi spremembami in zagotavljanje pravilnih in popolnih informacij,
- *razpoložljivost (ang. availability)*: informacije so na voljo uporabnikom, kadar je to potrebno.

Zaupnost, celovitost in razpoložljivost informacij lahko igrajo zelo pomembno vlogo pri ohranjanju konkurenčnosti, denarnih tokov, dobičkonosnosti, usklajenosti z zakonskimi zahtevami ter pri ohranjanju komercialne podobe družbe. Pri tem je pomemben element ustrezna uporaba različnih varnostnih ukrepov. S strani ponudnika storitve je varnost zagotovljena tako, da sam nima niti dostopa niti vpogleda v podatke svojih uporabnikov (Palsit, 2016). Več o varnosti oblačnih storitev bo predstavljeno v prihodnjih poglavjih.

Seveda je potrebno omeniti (Gradišar, 2003, str. 277), da se varnost ne nanaša samo na strojno, programsko in drugo pomožno opremo, temveč tudi na procese, delovne

razmere in okolje. Informacijska tehnologija je pomembna, vendar varnost vedno temelji na dobri organizaciji in usposobljenosti zaposlenih. Varnosti informacijskih sistemov se je potrebno posvetiti na dnevni ravni, potrebno se je zavedati, da je varnost nepretrgana dejavnost, za katero morajo biti odgovorni vsi zaposleni. Za varnost vsekakor ne more biti odgovorna le določena tehnična služba ali oddelek, saj gre za sistematičen proces, ki zadeva celotno organizacijo. Varnost informacijskih sistemov zajema varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij, upošteva zakonska in druga določila, neprekinjeno poslovanje in okrevanje po nesreči ter vprašanja glede zasebnosti.

2.2. NAMEN IN CILJ MAGISTRSKEGA DELA

Magistrsko delo je namenjeno tako posameznikom kot organizacijam, ki uporabljajo oblačne storitve.

Cilji magistrskega dela so:

- izdelati pregled literature in analizirati človeške vidike varnosti v oblačnih storitvah,
- predstaviti najpomembnejše koncepte varnosti, ki so trenutno uveljavljeni in se dotikajo človeškega vidika varnosti,
- analizirati primere delovanja posameznikov in skupin, ki so povzročili varnostne incidente v oblačnih storitvah in s tem prizadeli bodisi posameznike bodisi organizacije,
- predlagati model usposabljanja zaposlenih za varno uporabo oblačnih storitev in zgodnjega zaznavanja nevarnega obnašanja zaposlenih pri uporabi oblačnih storitev,
- pripraviti enostaven primer spletnega usposabljanja zaposlenih za varno uporabo oblačnih storitev, ki bi bil lahko v pomoč vsem organizacijam, ki bodo taka izobraževanja izvajala.

2.3. PREGLED RELEVANTNE LITERATURE

2.3.1. OPREDELITEV POJMA

Definicija družbe Gartner (v Plummer, 2009) navaja, da so oblačne storitve način računalništva, kjer so prilagodljive (ang. *scalable*) informacijske zmožnosti dostopne več odjemalcem oz. kupcem s pomočjo tehnologije interneta. Tudi Marks & Lozano (2010, 27) navajata, da je računalništvo v oblaku dostop na zahtevo v virtualizirana informacijsko tehnološka (IT) sredstva, ki so nastanjena izven lastnega podatkovnega centra, ki se ga deli z drugimi. Je enostaven za uporabo, plačljiv preko naročnine in dostopen preko spleta. Namen in cilj računalništva v oblaku je predvsem omogočiti dostop do računalniških zmogljivosti iz katerekoli lokacije na ekonomičen, prilagodljiv in nadgradljiv način (Tomšič, 2011). Torej gre za prilagajanje računalniškega sistema in omrežja zahtevam uporabnika. Tudi Butina (2010, str. 2) navaja, da so oblačne storitve prav to, kar je informatika potrebovala že od samega začetka, torej način, kako v trenutku povečati zmogljivost ali kapaciteto, ne da bi investirali v novo infrastrukturo, osebje ali licence. Omenja tudi, da oblačne storitve obsegajo različne storitve, ki v realnem času preko interneta povečujejo obstoječe zmogljivosti informacijskih tehnologij, plačujejo pa se z mesečno naročnino ali pa glede na porabo.

Kar nekaj avtorjev (Carr, 2009, str. 59; MacMillan Dictionary, 2009) je omenilo, da naj bi nov način ponujanja računalniških storitev in virov omenil leta 1961 že John McCarthy, saj je napovedal, da bo računalništvo nekoč organizirano kot javna storitev, podobno kot telefonija.

Willis (2008) navaja tri prelomne letnice, ko je bil termin oblačne storitve prvič uporabljen:

- 1997 (maj): podjetje NetCentric je želelo izraz patentirati, vendar tega ni realiziralo,
- 2001 (april): John Markoff je objavil članek in v njem uporabil besedno zvezo »oblak računalnikov«,
- 2006 (avgust): na Googlovi konferenci je sedanji predsednik uprave Googla Eric Schmidt uporabil izraz računalništvo v oblaku.

Geelan (2010) pa trdi, da je bil termin izumljen 24. februarja 2007, ko je bil napovedan CloudExpo, to je konferenca, ki se je osredotočala na pokrivanje predvsem poslovnih vidikov oblačnih storitev.

2.3.2. BISTVENE ZNAČILNOSTI, STORITVENI IN IZVEDBENI MODELI OBLAČNIH STORITEV

Kot smo že omenili, oblačne storitve odlikuje 5 bistvenih značilnosti, 3 storitveni modeli in 4 izvedbeni modeli, ki jih bomo v nadaljevanju podrobneje opredelili.

Na podlagi opredelitve Ameriškega Nacionalnega inštituta za standarde in tehnologijo (ang. *National Institute of Standards and Technology*, *NIST*) bomo opredelili 5 temeljnih značilnosti oblačnih storitev (Mell & Grance, 2009):

- *možnost samopostrežbe na zahtevo*: odjemalec oblačnih storitev lahko po potrebi sam spreminja računalniške zmogljivosti oz. vire (npr. velikost prostora na strežniku, št. Procesorjev, itd.), ki jih najema od ponudnika, in to brez njegovega poseganja;
- *širok dostop preko omrežja*: v tem primeru so zmogljivosti preko omrežja na voljo tako lahkim kot tudi težkim odjemalcem ter dostopne preko standardnih mehanizmov. Omenimo lahko, da so lahki odjemalci tisti računalniki in računalniški programi, ki so za opravljanje svojih osnovnih dejanj zelo odvisni od drugih računalnikov, težki odjemalci (strežniki) pa ta dejanja opravljajo sami;
- *združevanje virov*: fizični in virtualni viri ponudnika so združeni, da služijo več odjemalcem, katerim se dinamično dodeljujejo glede na njihovo potrebo po načelu večodjemalskega modela (ang. *multi-tenant*). Carr (2009, str. 77) primerja omenjeni model z večnadstropno stanovanjsko zgradbo. V osnovnem modelu, kjer sta le odjemalec-strežnik, biva le en stanovalec, torej prostor ostaja neizrabljen. V večodjemalskem modelu pa se stavba razdeli na posamezna stanovanja, ki jih najema več stanovalcev. Stanovalci so v posameznih stanovanjskih enotah svobodni, delijo pa si skupno fizično infrastrukturo in stroške. Največkrat stranka nima nadzora in informacij o tem, kje točno se nahajajo viri, lahko pa ve, v kateri državi, pokrajini in podatkovnem centru se nahajajo;
- *hitra prilagodljivost*: zmogljivosti se lahko zagotovijo hitro in prilagodljivo, v določenih primerih avtomatično, za hitro prilagajanje potrebam stranke, ki se jim tako lahko dozdeva, da so viri na voljo kadar koli in v neomejenih količinah;
- *merljiva storitev*: sistemi v oblaku avtomatično nadzirajo in optimizirajo uporabo virov z merljivimi zmogljivostmi, primernimi glede na vrsto storitve. Z opazovanjem, nadziranjem in poročanjem o uporabi virov se zagotavlja transparentnost tako za ponudnika kot odjemalca storitev.

V vodiču BITKOMA (2009) lahko zasledimo, da veljajo za pravo storitev v oblaku naslednje značilnosti:

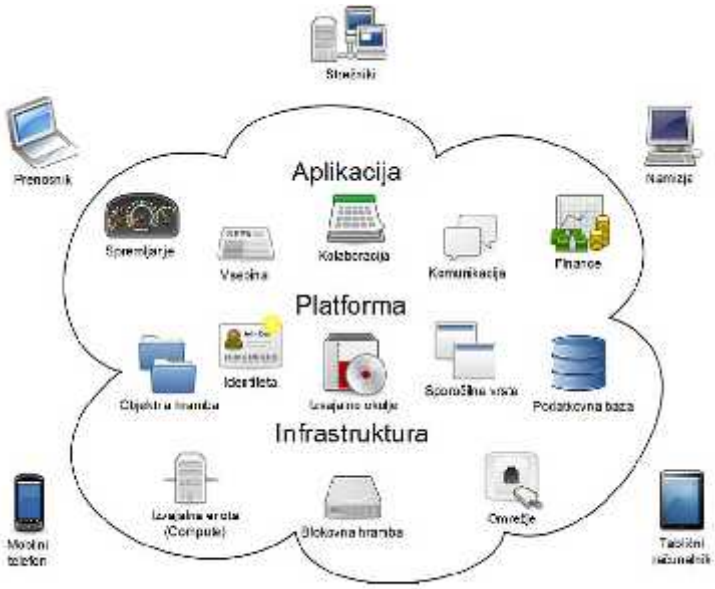
- *virtualni viri*: fizična izvedba storitve je uporabniku skrita. To izvajalcu omogoča, da optimizira storitve glede učinkovitosti in standardizacije;
- *sposobnost biti stranka*: v okolju s skupno rabo so posamezni viri namenjeni več uporabnikom, pri čemer se uporabljajo mehanizmi za zaščito in izolacijo vsake stranke, kar omogoča ponudniku, da izkoristi različne načine delovanja;
- *plačilo na osnovi porabe*: uporabnik plačuje samo za vire, ki jih dejansko tudi uporablja;
- *uporabnik ima nadzor nad uporabo*: uporabnik lahko sam naroči vire in uporaba se nato omogoči samodejno brez posredovanja ponudnika storitve;
- *elastičnost*: storitve se lahko spontano in hitro prilagodijo spremembam obremenitve. Uporabnik ima občutek, da so viri neskončni;

- *programski nadzor*: s pomočjo vmesnikov za programiranje lahko uporabnik nastavi vire, jih uporablja in upravlja. Tako lahko uporabnik na dinamičen način upravlja uporabo aplikacije, ponudniku pa je omogočena avtomatizacija upravljanja virov.

Tudi Simončič (2010) navaja, da so v strokovnih krogih sklopi delitev bolj dodelani in med seboj ločeni po karakteristikah delovanja. V teoriji in praksi pa je najpogosteje zaslediti, da oblačne storitve sestavljajo tri »plasti« oz. storitveni modeli. Kot omenjajo različni avtorji (Mell & Grance, 2009, str. 2; Jurič etal., 2009, str. 2; Sheehan, 2009; Čehovin, 2011) so to:

- *Infrastruktura kot storitev* (IaaS, ang. *Infrastructure as a Service)*, nam omogoča uporabo virtualiziranih virov, kot so procesorski čas, pomnilnik in diskovni prostor. Na infrastrukturi, ki jo najemamo, lahko uporabljamo operacijske sisteme in programske rešitve (ang. *application*, v nadaljevanju PR) po lastnih željah, podobno kot bi jih uporabljali na lastnem strežniku. Glavna prednost IaaS je, da lahko kapacitete prilagodljivo povečujemo ali zmanjšujemo. Vzdrževanje strojne opreme ni potrebno. Slabost je, da je IaaS lahko dražji kot ostale plasti. Nadzor in upravljanje zahtevata primerno usposobljene ljudi in sta lahko zahtevna (odvisno od ponudnika oz. storitve). Primeri IaaS so Amazon Web Services, GoGrid, Rackspace Cloud in drugi.
- *Platforma kot storitev* (PaaS, ang. *Platform as a Service)*, z uporabo programskih jezikov in orodij, ki jih je razvil ponudnik, uporabnik na platformi razvija in uporablja PR, ki jih je razvil sam oz. kupil od ponudnika. Glavna prednost je, da z najemom platforme v oblaku nista potrebna nameščanje in vzdrževanje operacijskega sistema in vseh ostalih programskih strežnikov (spletni, programski, podatkovni, procesni strežniki itd.), ki so potrebni v sodobnih informacijskih sistemih. Hkrati je lahko to tudi slabost modela PaaS, ker z večjim nadzorom nad razvijalskim okoljem izgubimo (oz. razvijalci PR) nadzor nad spodaj ležečo infrastrukturo ter postanemo odvisni od vzdrževanja in posodabljanja ponudnika. Primeri PaaS so Force.com (Salesforce), Google App Engine, Microsoft Azure in drugi.
- *Programska oprema kot storitev* (SaaS. ang. *Software as a Service)*, zagotavljanje programske opreme, naložene v oblaku. Uporabnik ima zelo omejen nadzor nad uporabo oz. nastavitvami PR in nima nadzora nad spodaj ležečo infrastrukturo in operacijskim sistemom. Uporabniku ni treba posodabljati PR, to počne ponudnik. Prednosti so dostopnost preko interneta, bogati vmesniki, pogosto brezplačna uporaba oz. plačilo po porabi ali z licencami (1 sedež oz. 1 oseba je 1 licenca). Slabosti so malo oz. nič možnosti prilagajanja po meri in omejeno število funkcij. Primeri SaaS so CRM (Salesforce.com), Gmail (Google) in drugi.

Abstraktni prikaz koncepta računalništva v oblaku s tremi storitvenimi modeli povzet po Varstvu osebnih podatkov in računalništvu v oblakih (2012) je prikazan na Sliki 1:



Slika 1: Abstraktni prikaz koncepta računalništva v oblaku. Povzeto po »Varstvo osebnih podatkov in računalništvo v oblakih«, 2012, str. 7

Tabela 1: Tipizacija storitev v oblaku (NIST in IBM)

Termin	**Definicija**
PaaS Vir: IBM	Poslovni proces kot storitev je kateri koli poslovni proces (horizontalni ali vertikalni), ki je izveden v okviru modela oblaka (multi-odjemalec, samopostrežno omogočanje uporabe, elastično spreminjanje meril in merjenje porabe ali cen) prek spletnih vmesnikov in ki uporablja spletno orientirano arhitekturo oblaka. Ponudnik PaaS je odgovoren za povezane poslovne funkcije.
SaaS Vir; NIST	Uporabnik lahko uporablja aplikacije, ki se izvajajo v ponudnikovi infrastrukturi v oblaku in so dostopne prek različnih odjemalnih naprav z vmesnikom za lahke odjemalce, kot je spletni brskalnik (npr. spletna elektronska pošta). Ne more pa upravljati ali nadzirati osnovne infrastrukture v oblaku, omrežja, strežnikov, operacijskih sistemov, pomnilnika ali posameznih aplikacij. Izjeme so možne pri omejenih uporabnikovih nastavitvah konfiguracije aplikacij.
PaaS Vir: NIST	Uporabnik lahko na infrastrukturo v oblaku postavi aplikacije, ki jih je sam ustvaril in ki podpirajo ponudnike, programske jezike in orodja (npr. JAVA, PYTHON, .NET). Ne more upravljati ali nadzirati osnovne infrastrukture v oblaku, omrežja, strežnikov, operacijskih sistemov ali pomnilnika, ima pa nadzor nad postavljenimi aplikacijami in potencialno konfiguracijami okolja, ki gostuje aplikacije.
laaS Vir NIST	Uporabnik ima možnost najema procesorske moči, pomnilnika, omrežja in drugih temeljnih računalniških sredstev; kjer lahko postavi in izvaja poljubno programsko opremo, kar lahko zajema operacijske sisteme in aplikacije. Ne more upravljati s temeljno infrastrukturo oblaka, ima pa nadzor nad operacijskimi sistemi, pomnilnikom, postavljenimi aplikacijami in lahko izbira omrežne komponente (npr. požarne zidove, programe za uravnavanje obremenitve).

Sčasoma so nastali tudi različni izvedbeni modeli oblakov (ang. *deployment models*). Kot navaja tudi Tomšič (2011), je bistvena značilnost računalništva v oblaku ta, da obdelava podatkov ne poteka na vnaprej določenem statičnem mestu, ločimo pa med javnimi, zasebnimi, skupnostnimi in hibridnimi oblaki. Prva dva tipa, javni in zasebni oblak, imata vsak svoje značilnosti, druga dva tipa, hibridni in skupnostni pa predstavljata združitev in kombinacijo javnega ter zasebnega oblaka. Nekateri avtorji Höllwarth (2012) omenjajo, da je bilo računalništvo v oblaku že kmalu razdeljeno na dve značilni pojavni obliki (praobliki), ki imata skupne določene lastnosti ali značilnosti. Konkretno je bila s tem mišljena splošna delitev v »zasebno« in »javno računalništvo v oblaku«. Novejše objave poleg dveh praoblik omenjajo še druge »modele postavitve (angl. *deployment models*)«, npr. »hibridni oblak (angl. *Hybrid Cloud*)« ali »oblak skupnosti (angl. *Communities Cloud*)«.

Različni avtorji (Voorsluys, Broberg in Buyya, 2011; Tomšič, 2011; Marks & Lozano, 2010, str. 37-38, Höllwarth, 2012, str. 38-43) opredeljujejo izvedbene modele takole:

- *Javni oblak* pomeni infrastrukturo, ki je namenjena splošni javnosti, skupnosti ali industrijski skupini, in je v lasti organizacije, ki ponuja oz. prodaja storitve v oblaku. Pogosto se pojem »oblak« uporablja kot sinonim za »javni oblak«. Javni oblaki so po naravi viri, ki so dostopni vsem, zato se pojavljajo vprašanja glede varnosti, prava in dostopnosti. Prednosti tega modela so vidne za podjetja, ki ne želijo vlagati v lastno IT in bi hkrati rada prihranila, saj se je tako možno vnaprej izogniti naložbam oz. jih na osnovi porabe spreminjati v stroške izvedbe. Slabosti tega modela pa se kažejo predvsem v večjih tveganjih. Številni pomisleki se pojavljajo tudi glede skladnosti, varnosti, dostopnosti, pa tudi zmogljivosti, ki jo je treba natančno preveriti za vsak posamezen primer.
- *Skupnostni oblak je* namenjen eni skupnosti, ki je sestavljena iz več organizacij, ki si med seboj zaradi skupnega interesa zaupajo. Lahko so v lasti ene ali več organizacij ali pa zunanjega ponudnika.
- *Zasebni oblak* je infrastruktura, namenjena izključno posamezni organizaciji, torej to pomeni zagotovitev oblačnih storitev znotraj zaprtega omrežja, npr. znotraj intraneta podjetja. Zasebni oblaki so ekskluzivni viri, neodvisni od lokacije, in so glede vprašanj o varnosti, pravu in dostopnosti bolj podobni tradicionalni IT. Ta tip oblaka upravlja organizacija sama ali pa ga upravlja zunanji ponudnik. Nameščen je znotraj posameznega centra organizacije in tako ustrezno zaščiten pred zunanjimi vplivi. Nahaja se lahko na lokaciji organizacije ali ponudnika. Prednosti tega modela so v individualnih prilagoditvah ter na področju varnosti in skladnosti. Bistvena slabost tega modela pa je, da vnaprej plačanih stroškov investicije pri tem modelu ni mogoče v celoti spremeniti v stroške izvedbe, saj mora podjetje vnaprej nabaviti in/ali sestaviti komponente za »zasebni oblak«, ki jih je nato pri dejanski rabi in obremenitvah mogoče nadgraditi.
- *Hibridni oblak:* infrastruktura je sestavljena iz dveh ali več oblakov (zasebni ali javni), ki kot taki tudi ostajajo še naprej, so pa medsebojno povezani s standardnimi tehnologijami, ki omogočajo prenosljivost aplikacij. Večina analitikov pričakuje, da se bodo v bližnji prihodnosti

najpogosteje uporabljale ravno implementacije v hibridnem oblaku, saj bodo podjetja lahko svoje storitve naročala modularno iz obeh svetov, »zasebnega« ali »javnega oblaka«, glede na prioriteto in občutljivost zahteve. Prednosti hibridnega oblaka so kombinacija fleksibilnosti javnega oblaka in zanesljivost zasebnega oblaka. Podjetje se tako lahko na zelo elastičen in dinamičen način odzove na vsa stanja obremenitve sistema in hkrati ohrani nadzor na vseh bistvenih področjih.

Računalništvo v oblaku ima veliko prednosti zaradi nižjih stroškov in odsotnosti potrebe po vložkih (nakup strojne opreme), večje in hitrejše prilagodljivosti potrebam naročnika (po potrebi možnost zakupa dodatne zmogljivosti), nižjih stroškov vzdrževanja ter drugih storitev in podpore, ki so vezane na IKT človeške vire. Pri določenih izvedbenih modelih je pogosto vse, kar uporabnik potrebuje, le dostop do interneta in brskalnik. Bistvene značilnosti računalništva v oblaku se lahko odrazijo tako v prednostih kot tudi slabostih, vsekakor pa so, kot je omenjeno v Smernicah (2011), povezane tudi s tveganji, ki niso značilna za druge oblike zunanjega izvajanja IKT storitev. Gartner (2011) omenja, da vrednost storitev v oblaku vsako leto skokovito narašča in naj bi po njegovem mnenju do leta 2015 narasla do 21,3 milijarde ameriških dolarjev.
Računalništvo v oblaku ima tako svoje prednosti in slabosti, ki jih opredeljujemo v tabeli 2.

Tabela 2: Prednosti in slabosti računalništva v oblaku (Zver 2011)

PREDNOSTI	**SLABOSTI**
nižji stroški	popolna odvisnost od omrežja
lažje vzdrževanje	izguba nadzora
višja računska moč	odzivnost in pasovna širina
virtualizacija	vprašljiva prenosljivost
hitrejši razvoj storitev in produktov	vprašljiva varnost
enostavno upravljanje	zakonodaja
dostopnost	zahtevna uvedba
nizki vstopni stroški	
manjši investicijski stroški (ni potrebno postavljati računalniške infrastrukture)	
plačamo le tisto, kar potrebujemo in uporabljamo	
enostavno povečanje virtualnih strojev	
hitre in učinkovite nadgradnje	

2.3.3. RANLJIVOST RAČUNALNIŠTVA V OBLAKU IN VARNOST

Vse, kar velja za varovanje vseh podatkov, ki jih želimo zaščititi, velja tudi za podatke v oblačnih storitvah, še prav posebej zato, ker je glavna značilnost oblaka, da vse poteka preko omrežja in prav zato so podatki še toliko bolj izpostavljeni vdorom nepooblaščenih uporabnikov, ki se na nedovoljen način želijo dokopati do informacij. V nadaljevanju se bomo osredotočili predvsem na varnost podatkov v oblačnih storitvah in kako jo vzdrževati.

Cachin in Schunter (2011) navajata, da stvari, ki so povezane z internetom, torej tudi računalništvo v oblaku, niso imune na varnostne probleme. Že v preteklosti se je izkazalo, da so imele oblačne storitve številne šibke točke, ki so jih napadalci s pridom izkoriščali. Kot navaja Božič (2011), je enostavnost in dostopnost storitev v oblaku dober razlog, da organizacije pričenjajo z uporabo teh storitev za različne namene, seveda pa je pri tem pomembno tudi vprašanje nadzora nad podatki in njihovo varnostjo. Varnost podatkov na spletu bi lahko opredelili tudi kot preprečevanje nepooblaščenim osebam, da bi dostopale in posegale po datotekah z zaupnimi podatki. Zaupne datoteke je možno blokirati z gesli, tak način varovanja informacij pa uporabljajo pravzaprav že vsi uporabniki tovrstnih storitev. Z najemom storitev v oblaku prenesemo podatke iz našega bolj ali manj varnega okolja, kjer lahko z različnimi varnostnimi postopki in metodami sami poskrbimo za varnost podatkov, na splet. Božič (2011, str. 9) omenja, da »poleg tega problema, da lahko zgradimo pravo trdnjavo na svojem lokalnem omrežju, nato pa vse podatke izvozimo v oblak, se trenutno kot morda največji problem kaže preveč enostavna avtentikacija. Z ukradenim geslom (ali drugim avtentikacijskim sredstvom) lahko napadalec naenkrat pride do širokega nabora storitev v oblaku. Oblačne storitve za enkrat še ne ponujajo bolj strukturiranega nadzora nad dostopom, preko katerega bi lahko opredelili več nivojev storitev in jih zaščitili z dodatnimi mehanizmi«.

Poleg gesel obstajajo tudi določena pravila, ki določajo način zaščite dokumentov. Imenujemo jih varnostni pravilnik. Varnostni pravilnik je skupek zakonov in predpisov, ki narekujejo, kako naj neka organizacija zavaruje, razporeja in upravlja občutljive informacije, ki jih želi zaščititi pred nepooblaščenim uporabnikom, poleg tega pa obsega tudi postopke nadzora dostopa, postopke nadzora pretoka informacij, itd. Omenjeni pravilnik nadzoruje nastavitve zaščite za dokument glede na stanje dokumenta v shrambi objektov in je sestavljen iz ene ali več predlog zaščite. Predloge definirajo zaščite za razred dokumenta glede na stanje različice dokumenta. Varnostni pravilnik pa mora upoštevati tudi zakonodajo o zaščiti podatkov (Pahor & Drobnič, 2002, str. 622). Naloga varnosti je torej predvsem varovanje podatkov, kadar se ti prenašajo po omrežju, in pa tudi sama zaščita računalniškega sistema pred nepooblaščenim dostopom nekega uporabnika.

Različni avtorji (Grobauer, Walloschek, Stocker, 2011) navajajo, da največje ranljivosti računalništva v oblaku izhajajo iz njegovih osnovnih karakteristik, in sicer:

- *Nedovoljen dostop do vmesnika za upravljanje (ang. unauthorized access to management interface):* za uporabo storitve na zahtevo potrebujemo

vmesnik, s katerim lahko uporabniki dostopajo do storitve. Vmesnik je tako kritična točka za varnost sistema oz. potencialna ranljivost, saj do nje dostopa veliko uporabnikov. V klasičnih sistemih pa do njega dostopa le nekaj administratorjev.

- *Ranljivost internetnega protokola*: storitve računalništva v oblaku morajo biti vedno na voljo. Navadno do njih dostopamo preko internetnega omrežja. Omrežje pa ni varno. Problem so predvsem »vrinjeni napadalci« (ang. *man in middle attack*).
- *Ranljivost obnovitve podatkov*: lastnost dinamičnega dodajanja virov lahko ustvari ranljivost, da so viri enega uporabnika dodeljeni drugemu uporabniku.
- *Merjenje in obračunavanje utaj (ang. Metering and billing evasion)*: računalništvo v oblaku uporablja meritve glede tega, koliko virov uporabljajo posamezni uporabniki za kasnejše obračunavanje (ang. *Pay per use*).

Med varnostna tveganja računalništva v oblaku sodijo obdelava osebnih podatkov kot tudi dostop do podatkov v oblaku s strani uporabnika in njihov izvoz. Ker oblačne storitve ponujajo uporabnikom PaaS in IaaS, lahko pride do kraje, zlorabe in nezakonite distribucije podatkov. Seveda se lahko tudi vprašamo, kot navaja Tomšič, (2011, str. 15-19), kaj se zgodi, ko uporabnik posreduje v javni oblak določene podatke in kakšna je njihova zaupnost, kot tudi ali ima sploh kontrolo nad svojimi podatki v oblaku. Med varnostna tveganja računalništva v oblaku sodi tudi sam problem lokacije podatkov in s tem tudi skupna hramba podatkov različnih uporabnikov, kot tudi vprašanje zagotavljanja podatkov le njihovim lastnikom.

Varnost distribuiranega sistema je, kot navaja Vidmar (2011, str. 226), kompleksno in zelo široko področje, ki ga rešujejo različni tehnološko-tehnični in splošno inženirski pristopi. Velikokrat se zgodi, da opredeljujemo varnost pravzaprav kot izključevanje nevarnosti, torej povedano z drugimi besedami, »govoriti o varnosti je zelo težko, če ne celo nesmiselno, če ne znamo ali ne moremo opredeliti nevarnosti.«

Na žalost je ozaveščenost uporabnikov o varnosti običajno na zelo nizki stopnji, hkrati pa moramo tudi omeniti, da pravzaprav absolutno varen sistema ne obstaja. Stopnja varnosti je odvisna predvsem od nevarnosti, ki sistemu in uporabnikom objektivno grozijo. Pri tem ne gre za imaginarnega notranjega ali zunanjega sovražnika, kot omenja Vidmar (2011), ampak moramo razlikovati med slabostmi tehnologije, ki odpoveduje ali deluje napačno, in napadi na sistem, ki jih vedno izvede človeški faktor kot napadalec. Varovanje mora biti usmerjeno v preprečevanje potencialno možnih odpovedi sistema, napačnega delovanja sistema ali napada na sistem. Veliko potencialnih nevarnosti lahko predvidimo ali identificiramo s kvalitetnim in zanesljivim nadzorom sistema, kar pomeni, da bi bil idealen rezultat nadzornega sistema varnost, ki sploh ne bi bila ogrožena in zato zaščitnih mehanizmov sploh ne bi potrebovali (Vidmar, 2011).

Varnost sistema, ki jo lahko definiramo kot odpornost na napake, ter zanesljivost in zaščito sistema lahko opazujemo na nivoju končnih računalnikov (lokalna varnost računalnika) in varnosti, ki je potrebna zaradi narave distribuiranega sistema (distribuirana varnost sistema). Varnostna področja delimo (Vidmar, 2011, str. 226-228) na: zanesljivost sistema, zaščito sistema ter nadzor in upravljanje, kar natančneje opredeljujemo v nadaljevanju.

Zanesljivost sistema pomeni zagotavljanje pogojev za delovanje storitev in normalno delo uporabnikov. Področje v najširšem smislu besede sodi v okvir sistemskega inženiringa. Zanesljivost opredeljuje segment varnosti, ki opredeljuje varnostno razmerje med uporabniki in sistemom. Zanesljivost je pogojena predvsem z:

- načrtovanjem in izvedbo sistema,
- vzdrževanjem ter
- servisiranjem sistema in na koncu, kar pa ni najmanj pomembno, z usposobljenostjo uporabnikov.

Zaščita sistema onemogoča izvajanje nelegalnih storitev, torej tistih, za katere sistem ni predviden. Poleg tega tudi preprečuje dostop do virov sistema neregularnim uporabnikom oz. vdiralcem. Naj omenimo, da je tako imenovani registriran uporabnik prav tako vdiralec, če deluje izven svoje uporabniške kvote oziroma pravic, ki mu jih dodeljuje upravljavec sistema. Zaščita opredeljuje varnost, ki jo določa razmerje med dejansko namembnostjo sistema ter predvideno namembno uporabo.

Zaščito delimo na:

- zaščito dostopa do sistema,
- zaščito sporočil v transportnem sistemu,
- zaščito integritete uporabnikov in
- zaščito integritete sporočil.

Nadzor in upravljanje tehnoloških, uporabniških in organizacijskih virov distribuiranega informacijskega sistema je tretja dimenzija, ki zagotavlja varnost sistema, in sicer ne glede na to, ali rešujemo probleme odpornosti na napake, zanesljivosti ali zaščite. Dober nadzor omogoča, kot navaja Vidmar (2011, str. 228), »da poznamo razmere in stanje sistema med delovanjem in posledično ustrezno ukrepamo, ko je varnost s stališča zanesljivosti ali zaščite ogrožena. Nadzirati sistem pomeni, da poznamo kvalitativne in kvantitativne lastnosti tehnologije v obratovanju, da nadzorujemo »obnašanje« uporabnikov in da pravočasno zaznamo kritične točke, ki lahko prizadenejo sistem.« Iz omenjenega je sklepati, da je nadzor in upravljanje sistema ter posledično tudi ustrezno ukrepanje sistema eden od glavnih dejavnikov zanesljivosti sistema. Nadzor sistema je potreben za ustrezno in kvalitetno vzdrževanje in servisiranje sistema ter za zagotavljanje potrebne varnosti sistema. Nadzor sistema pomeni določen proces, ki preverja pravice ostalih procesov ali uporabnikov za dostop do določenih podatkov in informacij (Brodnik et al. 1998, 101).

Za varnost računalništva v oblaku je potrebno upoštevati naslednjih dvajset varnostnih priporočil (Antonopoulos & Gilliam, 2010, 296):

1. Zagotoviti globalno edinstvena imena, ki z lahkoto omogočajo identifikacijo ključnih značilnosti atributov.
2. Zagotoviti zapise virov na posameznih lokacijah, tako fizično in virtualno, skozi celoten življenjski cikel in s tem omogočiti sledljivost podatkov.
3. Ne smemo kar tako zaupati oblaku v vseh primerih saj vsaka interakcija v oblaku zahteva dovoljenje in identifikacijo.
4. Priporočljivo je tudi šifriranje podatkov, še posebej takrat, ko jih prenašamo med strežniki.
5. Omejevanje dinamike uporabe sredstev na vnaprej določenih ravneh, da bi preprečili notranje napade na določene informacije.
6. Odstraniti podatke, ko niso več potrebni oziroma ko jih več ne rabimo.
7. Priporočljivo je tudi določiti prednostne naloge za vsak primer v oblaku, ki zagotavljajo ustrezno dostopnost in uporabo virov.
8. Posluževati se upravljalnega managementa, prijavnih postopkov ter nadzornega sistema, ki podpira celoten oblak.
9. Omejiti dostop do podatkov uporabnikom z določenim poslovnim namenom.
10. Ustvarjanje novih primerov v skladu z opredeljenimi, preizkušenimi in potrjenimi specifikacijami.
11. Izvajanje aplikacij na več fizičnih strežnikih za izboljšanje zanesljivosti.
12. Zagotavljanje centralizirane avtentikacije in avtorizacije storitev.
13. Zagotoviti centraliziran sistem upravljanja z občutljivimi informacijami.
14. Digitalno podpisovanje kontrolnih sporočil v oblaku z namenom preprečevanja ponarejanja in nepooblaščene uporabe.
15. Omejiti točke za vstop oziroma izstop podatkov v oblak za preprečitev uvedbe zlonamerne programske opreme in vdorov do zasebnih podatkov.
16. Zapis trenutnega stanja in evidentiranje fizičnih in virtualnih virov.
17. Izolirati sumljive primere in jih nadomestiti z alternativnimi.
18. Skeniranje oblaka, da bi ugotovili, osamili in odpravili nedovoljene primere.
19. Revizija uporabe virov za odkrivanje sumljivih dejavnosti v oblaku.
20. Revizija primerov kot so ustvarjanje, migracije, hibernacija in zagon za zagotavljanje skladnosti.

2.4. OMEJITVE RAZISKAVE

Varnost v oblaku je ves čas zaznamovana z velikimi tveganji, ta pa se nanašajo tako na osebne (lokacija in zdravstveni podatki) kot na finančne podatke, podatke o proizvodnji, procesih, dobaviteljih, prometu. Gre za neposredno izgubo, spreminjanje ali celo krajo podatkov. Človek pravzaprav ne ve, kaj je huje – kraja ali sprememba podatkov.

Ena izmed najbolj podcenjenih in hkrati najnevarnejših metod zlorabe človekovega zaupanja je socialni inženiring, ki je zlasti uspešen v povezavi z uporabo modernih tehnologij. Socialni inženiring po svoji naravi pomeni predvsem pridobivanje določenih koristi z zlorabo zaupanja posameznika oz. z manipulacijo. Gre za prakso, ki bo najverjetneje vse bolj pogosta, predvsem zaradi možnosti hitrega zaslužka s pomočjo internetnih goljufij in počasnih reakcij zakonodajalca. Informacijski pooblaščenec

(2009) navaja, da »socialni inženiring ogroža varnost informacij predvsem zaradi svoje sposobnosti zaobiti tehnična sredstva varovanja, saj se prvenstveno usmerja na človeka kot najšibkejši člen v verigi varovanja informacij«. Torej lahko rečemo, da »socialni inženiring z zlorabo zaupanja, z uporabo socialnih veščin oziroma psiholoških tehnik, kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva in podobno, pridobi od žrtve osebne podatke (najpogosteje ime, priimek, št. transakcijskega računa, razna gesla, EMŠO, št. potnega lista) in jih uporabi za pridobivanje večinoma premoženjske koristi« (informacijski pooblaščenec, 2009). Pri socialnem inženiringu gre za še eno metodo, s katero napadalec prodre v varovano omrežje. V tej zvrsti napada igra glavno vlogo človek, ki zaradi pomanjkanja računalniškega znanja in prevelikega zaupanja napadalcu omogoči vstop v omrežje. Najbolj razširjene metode socialnega inženiringa so:

- prijateljstvo (vstopna gesla se pridobi na osnovi zaupanja med zaposlenimi);
- elektronska pošta (ponarejanje naslova pošiljatelja);
- pregledovanje smeti (pregled smeti podjetja lahko razkrije uporabne informacije);
- pregled pisarn (napadalec vohlja po odklenjenih pisarnah in kabinetih);
- zloraba zaupanja (napadalec si pridobi zaupanje zaposlenih);
- čas (element, ki je vedno na strani napadalca).

Najboljša obramba pred takimi napadi je, kot omenja Bratuša (2006, str. 241-242), »prav gotovo redno usposabljanje zaposlenih, ki jim je treba praktično ponazoriti, na kaj morajo biti pri delu pozorni in kateri podatki so še posebej pomembni. Poleg tega je zelo pomembno, da podjetje prilagodi varnostno politiko takim napadom, saj v nasprotnem primeru požarni zidovi in sistemi IDS ne zagotavljajo nikakršne varnosti«.

Kljub temu, da je koncept usposabljanja in zgodnje detekcije nevarnega obnašanja zaposlenih izredno visokega pomena, vidimo eno izmed omejitev raziskave v majhnem številu dostopnih empiričnih študij, ki bi lahko odgovorile na vprašanje, kako oblikovati tovrsten model. Izbrali smo si področje, ki še ni dovolj raziskano in tako se lahko zgodi, da bo strokovna literatura omejena.

3. PREGLED UPORABE OBLAČNIH STORITEV

3.1. POSAMEZNIKI

V zasebnem svetu posamezniki pogosto uporabljajo storitve, za katere se niti ne zavedajo, da delujejo kot oblačna storitev. Kot primer lahko navedemo elektronsko pošto Gmail, ki deluje transparentno za končnega uporabnika. Pohorec (2011) omenja, da je taka storitev transparentna v smislu, da se uporabnik ne zaveda strojne in programske opreme, ki mu omogočata dostop do pošte, saj ga zanimata samo raven kakovosti storitve (morebitna nedosegljivost) in velikost poštnega predala.

Največji problem, s katerim se danes tehnologija oblačnih storitev srečuje, je prav gotovo nepoznavanje in nezaupanje uporabnikov v samo tehnologijo. Kljub temu pa moramo omeniti, da se je v relativno kratkem času svojega obstoja uspela razširiti in integrirati v številne programske sisteme in različne aplikacije, ki so v množični uporabi. Številni uporabniki oblačnih storitev se pravzaprav niti ne zavedajo, da z uporabo strežnika za elektronsko pošto Gmail ali družbenega omrežja Facebook pravzaprav uporabljajo brezplačno obliko tehnologije podatkovnega oblaka. Med najbolj poznane in uporabljene storitve tehnologije podatkovnega oblaka uvrščamo spletne e-poštne storitve (npr.: Gmail, Hotmail, Yahoo), družbena omrežja (Facebook, Twitter, Linkedin, Google+), aplikacije za shranjevanje podatkov na spletu (Dropbox, GoGrid), "spletne pisarne" (Google Docs, MS Office, Live Meeting), aplikacije za objavo slik in videov (Picasa, Youtube) in številne druge (Simčič 2011).

Simčič (2011) omenja tudi, da sedaj večina ljudi uporablja več tehnoloških naprav za delo in prosti čas, pri tem pa igra ravno tehnologija podatkovnega oblaka ključno vlogo, saj želijo imeti uporabniki svoje podatke na dosegu roke v vsakem trenutku.

3.2. OBLAČNE STORITVE V BANČNIŠTVU

Majcen Velečič (2012) omenja, da je »skozi čas bančna industrija doživljala velike spremembe. Kljub dolgi zgodovini bančništva, ki sega tisočletja pred naše štetje, je ravno v zadnjem času prišlo do spremembe, kot je bančna industrija še ni doživela. Tokrat ne gre za spremembo, ki bi bila posledica poslovnega okolja banke, ampak za spremembo, ki se zdi bančnemu sektorju izjemno kompleksna. Ta sprememba izvira iz informacijsko tehnološke panoge, ki bančno industrijo spremlja že od obdobja po prvi svetovni vojni. Sprememba prihaja na krilih oblakov«.

Hőllwarth (2012) navaja, da mora imeti banka, ki iznaša podatke, stalen nadzor nad svojo osrednjo dejavnostjo. V zvezi z računalništvom v oblaku je zelo pomembno, da hrambo podatkov vedno razumemo kot iznos/zunanje izvajanje. Zaradi tega so potrebna stroga pravila. Kot primer lahko navedemo, kako je to zagotovljeno v Nemčiji, Avstriji in Švici:

- Nemčija: zvezni zavod za nadzor finančnih storitev nadzira dejavnost tako, da določa načela v »Minimalnih zahtevah za obvladovanje tveganj«;

- Avstrija: avstrijski organ za finančni trg nadzira dejavnost tako, da določa splošna načela v vodiču »Obvladovanje operativnega tveganja« in z objavo »Načela pravilne skladnosti«;
- Švica: švicarski organ za finančni trg (FINMA) nadzira dejavnost tako, da določa načela v okrožnici »Zunanje izvajanje poslovnih dejavnosti bank«.

Banke so zaradi narave svojega dela veliko vlagale v razvoj informacijskih sistemov, vendar se je velikokrat izkazalo, da še posebej v oblačnih storitvah vlogo informatikov v celoti prevzemajo zunanji izvajalci, kar pa seveda pomeni tveganje glede varnosti. Zaradi varnosti se poraja tudi pomislek pri odločanju za prehod v oblak. Pri vprašanju varnosti gre predvsem za pravice vpogleda v podatke v smislu administratorjev sistema, skladnosti z regulativo glede zunanjih revizij, hranjenja in upravljanja podatkov v skladu s politiko zasebnosti, segregacijo podatkov, nadomestne lokacije v primeru nesreče neodvisno od platforme, zagotavljanje odkrivanja nezakonitih dejavnosti in dolgoročno zagotavljanje delovanja (Majcen Velečič, 2012).

Kot primer lahko omenimo kibernetsko kriminaliteto in sicer goljufije povezane s plačilnim prometom, kjer storilci praviloma izrabljajo šibke točke digitalnih plačnih transakcij, med drugim (Bankart, 2015):

- goljufije, povezane s plačilnimi (debetnimi, kreditnimi, itd.) karticami in napadi na POS-terminale (angl. *point of sale attack*). POS-terminal je naprava, ki omogoča izvedbo plačilne transakcije s plačilno kartico. Neposredni strošek kartičnega poslovanja sta najemnina POS-terminala in plačilo provizije po posamezni transakciji ponudniku teh storitev;
- napade na sisteme mobilnega plačevanja s pametnimi telefoni s tehnologijo NFC (na primer, v Sloveniji plačilo vozovnice Ljubljanskega potniškega prometa z aplikacijo na pametnem telefonu);
- goljufije, povezane s kriptovalutami (na primer bitcoin).

Fiorletta (2012) opozarja, da je zaradi naraščanja uporabe plačilnih in kreditnih kartic za plačevanje na POS-terminalih mogoče pridobiti dostop do podatkov plačilnih kartic in PIN-številk pri POS-terminalih. Goljufije, povezane s POS-terminali, obsegajo napade na bankomate, ročne POS-terminale (povezane bodisi brezžično po mobilnem omrežju GSM bodisi prek ponudnikov kabelskega interneta) ali pa podatkovne zbirke (na primer pri prodajalcih). Raziskava o varnostnih tveganjih potrošnikov (Majcen Velečič, 2012) kaže, da je več kot 45% uporabnikov, ki svoje finance urejajo po internetu prepričanih, da jim bo banka v primeru kraje denarja s spletnega računa denar povrnila. Tovrstno zaupanje potrošnikov lahko slabo vpliva na poslovanje finančnih organizacij, ki v primeru spletne tatvine utrpijo škodo tako glede financ kot ugleda.

Trenutna gospodarska kriza od bank zahteva, da so fleksibilne, še posebej v znižanju stroškov informacijske tehnologije, vendar ne za ceno kakovosti. Nižji stroški informatike se kažejo kot najbolj očitna prednost računalništva v oblaku. Vsekakor pa bančništvo v oblaku prinaša kompleksne spremembe tako z vidika procesov v banki kakor tudi z vidika strank. Različne banke z uvajanjem najsodobnejših tehnologij bančnega poslovanja svojim strankam nudijo celovite bančne in finančne storitve

najvišje kakovosti, tako doma kot tudi v tujini. Zagotavljajo jim tako osebne in specializirane bančne storitve na bančnih okencih, kot tudi sodobno elektronsko bančništvo, ki se ga lahko stranke poslužujejo doma ali na delovnem mestu. Z oblačnimi storitvami si tako zmanjšajo stroške, kar je eden bistvenih razlogov za uvedbo oblačnih storitev, hkrati pa zagotavljajo varno, donosno, hitro ter prilagodljivo bančno poslovanje. Ker so banke močno odvisne od svojih strank, ki so lahko skeptične glede lokacije hranjenja podatkov in zagotavljanja varnosti za svoje podatke, je zagotavljanje usklajenosti z zakonskimi zahtevami še kako pomembno. Sem štejemo tudi zagotavljanje varnosti podatkov, k čemer je banka zavezana še posebej, ko govorimo o oblačnih storitvah.

V nadaljevanju bomo predstavili glavne prednosti oblaka za banko, kot jih izpostavlja Majcen Velečič (2012):

- storitve se obračunavajo po uporabi,
- banka se lažje in hitreje prilagaja potrebam strank, saj produkte in storitve hitreje ponudi strankam,
- banka se lahko bolj posveča oblikovanju in ponudbi bančnih storitev na račun zmanjšane osredotočenosti na informacijsko tehnologijo,
- tveganja izpadov so prenesena na izvajalca,
- naročnik ni vezan na samo en oblak, ampak lahko najema storitve pri različnih ponudnikih.

Raziskave kažejo, da finančne institucije vidijo največje potenciale oblačnih storitev v znižanju stroškov, hitrejšem času, hitrem prodoru produktov in storitev na trg, večji prilagodljivosti, kot tudi hitrem obračunavanju provizij (Majcen Velečič, 2012). V sklopu teh raziskav je 69% anketiranih izjavilo, da jim bo računalništvo v oblaku pomagalo doseči večjo fleksibilnost, prav tako pa jih polovica meni, da tehnologija pomeni konkurenčno prednost in omogočanje inovacij. Poleg tega v finančnih institucijah (Sudhir, 2011) izpostavljajo prednosti oblaka v neprestanem izboljševanju programske opreme, novih poslovnih priložnostih in večji možnosti za trženjske dogodke. Kljub vsem prednostim, ki jih nudi oblak, ne gre pozabiti na potrebno analizo, ki jo velja opraviti pred izborom izvajalca, saj je pomembno, da si lahko odgovorimo na vprašanje, kaj želimo z oblačnimi storitvami doseči in v kašni meri se bo s tem izboljšalo naše finančno poslovanje. Vsekakor pa pri tem ne smemo pozabiti na varnost.

Spodnji model (Markelj & Bernik, 2011) prikazuje (Slika 2) enega od možnih načinov sistematične vpeljave oblaka v organizacijo. Zelo pomembno je, da najprej že znotraj obstoječega informacijskega sistema ugotovimo, zakaj bomo storitev oblak uporabljali. Zaradi prenosa in hranjenja podatkov ali zaradi uporabe aplikacij, ki nam jih ponudnik nudi, ali morda kar obojega. Na podlagi omenjenih informacij in informacij, ki jih pridobimo z oceno informacijskega tveganja (informacije, programska oprema, itd..), kot omenjata avtorja, lahko pričnemo z izborom tipa oblaka in možnih ponudnikov. Pri izboru tipa oblaka je zelo pomembno, da sodelujejo vse organizacijske strukture organizacije kot tudi pomembni ključni kadri za informacijsko varnost.

S preudarnim in sistematičnim izborom oblaka, ki upošteva tudi zahteve informacijske varnosti, zmanjšamo verjetnost vpliva kombiniranih groženj na informacijski sistem organizacije (Markelj & Bernik, 2011).

Slika 2: Model izbora tipa oblaka (Markelj & Bernik 2011)

3.2.1. VARNOST OBLAČNIH STORITEV V BANČNIŠTVU

Pomembno je še, kot omenjata (Markelj & Bernik, 2011), da vsakokrat, ko implementiramo novo tehnologijo, kot v primeru računalništva v oblaku, zastavimo temelje informacijske varnosti že v fazi načrtovanja sistema. Zelo pomembno je, da organizacija analizira svoje procese, jih po potrebi posodobi in usposobi svoje zaposlene. V primeru postavitve procesa, ki se postavlja na novo ali se posodablja zaradi vpeljave računalništva v oblaku, je vsekakor zelo pomembno, da se v to vključijo vsi poglavitnimi udeleženci, saj šele tako lahko dosežejo optimizacijo, boljše in hitrejše prilagajanje in seveda višjo stopnjo varnosti.

Vzroki za nevarnosti in tveganja v zvezi z informacijskimi viri, kot jih navajajo različni avtorji (Gradišar et al., 2005, str. 295), so: napačno ravnanje človeka, različne strojne okvare, napake v programih, napake v podatkih, poškodbe računalniške opreme, neprimerne tehnične karakteristike in neodgovornost. V primeru ogrožene varnosti lahko pride do katastrofalnih posledic. V nadaljevanju bomo podrobneje opredelili pomanjkljivo oziroma napačno ravnanje človeka.

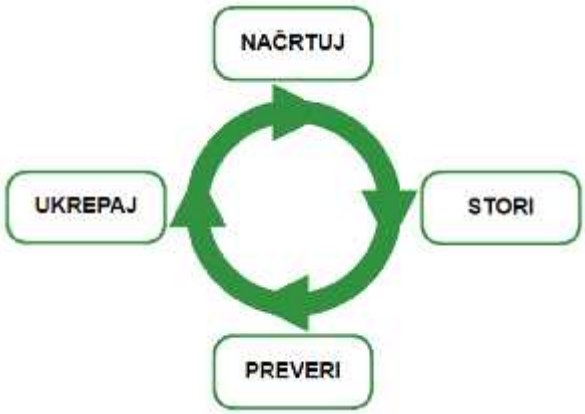
Človek lahko napačno ravna tudi zaradi neodgovornosti, saj lahko rečemo, da odgovornost pomeni, da nekdo odgovarja za svoja dejanja oziroma svoje izdelke in storitve. Odgovornost je tem večja, čim večjo škodo ali korist lahko nekdo s svojim ravnanjem povzroči. Do nesreč prihaja, ker v praksi posamezniki svoje odgovornosti ne uresničujejo, oziroma se obnašajo neodgovorno. Do nesreč pa lahko prihaja tudi, kot smo že omenili, s socialnim inženiringom z zlorabo zaupanja, torej z uporabo socialnih

veščin oziroma psiholoških tehnik, s pomočjo katerih se pridobi od žrtve npr. osebne podatke, ki se jih nato uporabi za pridobivanje večinoma finančnih koristi. Na podlagi omenjenega lahko zaključimo, da smo ljudje z vidika varnosti eden najšibkejših členov informacijskih sistemov.

Tako smo torej priča nenehnemu uhajanju informacij, predvsem po zaslugi človeka. Leskovar (2011) si na primeru varovanja zdravstvenih podatkov v oblaku zastavlja vprašanje, koga zanimajo podatki in v kakšnem primeru, kar pa bo verjetno vedno bolj aktualno vprašanje tudi za druga področja. Prav zaradi različnih groženj uhajanja podatkov oz. informacij v različnih organizacijah uvajajo različne sisteme varovanja informacij.

Varnost informacijskih sistemov in varnost podatkov ter informacij je z razmahom elektronskih komunikacij postala eden glavnih dejavnikov pri izvajanju dejavnosti bank. Problema varovanja informacij se zaradi različnih oblik informacij ne da reševati samo s tehničnimi ukrepi, zato je potreben celovit pristop tako v okviru informacijske tehnologije kot tudi z drugimi ukrepi, postopki, standardi, kontrolami in nadzorom.

Kot primer naj omenimo (Brezavšček& Moškon, 2010) sistem SUVI (Slika 4) ali (ang. ISMS – *information security management system*), ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju varovanja informacij. SUVI je bil vpeljan po standardih SIST ISO/IEC 27001:2006 in SIST ISO/IEC 27002: 2008. Temeljiti mora na ciljih, ki jih organizacija želi doseči z varovanjem in zaščito, na izbiri ustrezne strategije, ki bo ustrezala velikosti podjetja, na načinu in obsegu poslovanja, sredstvih, organizacijski kulturi ter znanju. SUVI za vzpostavitev in upravljanje uporablja procesni pristop, ki temelji na tako imenovanem NSPU modelu Demingovega kroga, in sicer v štirih fazah: načrtuj – stori – preveri in ukrepaj (Slika 3):



Slika 3: Demingov krog (SIST ISO/IEC 27001) (Brezavšček in Moškon 2010)

Uvedba in upravljanje sistema za upravljanje varovanja informacij poteka po procesnem pristopu in sicer v štirih fazah.

V nadaljevanju bomo omenjene faze natančneje opredelili (Brezavšček & Moškon, 2010, str. 101-107):

1. faza – NAČRTUJ – vzpostavitev SUVI
V tej fazi je potrebno zagotoviti jasno definiranje ciljev in zahtevanega nivoja varovanja informacij. Izhajati je potrebno iz osnovne zahteve, da mora informacijski sistem zagotavljati in podpirati učinkovito izvajanje vseh in še posebej ključnih poslovnih procesov v organizaciji. Natančno in jasno je potrebno opredeliti varnostna tveganja z namenom preprečevanja nedelovanja oziroma okrnjenega delovanja informacijskega sistema. Izvedba analize in ocene tveganj je osnova za določitev okvira SUVI, ki je v vsaki organizaciji drugačen glede na njeno specifičnost, pomembnost in odvisnost od informacijskega sistema za izvajanje poslovnih procesov. Ključni del prve faze vzpostavitve SUVI pa je izdelava načrta vzpostavitve in kar je najpomembneje, sprejem in potrditev načrta s strani najvišjega vodstva organizacije.

Prva faza vzpostavitve SUVI vključuje naslednje aktivnosti:
- izvedba analize in ocene varnostnih tveganj za vse ključne poslovne procese v organizaciji,
- na podlagi ocene tveganj sledi določitev okvira SUVI,
- izdelava načrta vzpostavitve SUVI v organizaciji,
- sprejem odločitve vodstva organizacije za pristop k projektu SUVI.

2. faza – STORI – vpeljava in delovanje SUVI
Na osnovi sprejetega načrta vzpostavitve SUVI sledi uvedba SUVI v organizacijo. Krovni dokument izvedbe celotnega projekta vzpostavitve SUVI in vodilo za njegovo uvedbo je politika varovanja podatkov in informacij, ki ga sprejema in potrjuje najvišje vodstvo organizacije. Glede na to, da je politika okviren dokument, je potrebno izdelati in potrditi izvedbene dokumente na več nivojih, vse do najnižjega nivoja, ki zagotavlja operativno izvajanje vseh potrebnih aktivnosti za doseganje zahtevanega nivoja varovanja informacij. Sprejeti izvedbeni dokumenti so osnova za aktivnosti uvajanja SUVI, kar pomeni informiranje in izobraževanje vseh zaposlenih kot tudi zunanjih sodelavcev in pogodbenih partnerjev organizacije.

Uvedba SUVI vključuje naslednje aktivnosti:
- izdelava in sprejem politike varovanja podatkov in informacij s strani najvišjega vodstva organizacije,
- izdelava, potrditev in sprejem izvedbenih dokumentov SUVI,
- uvedba SUVI (politike in izvedbeni dokumenti),
- seznanjanje in izobraževanje vseh zaposlenih, zunanjih sodelavcev in pogodbenih partnerjev organizacije, ki pri svojem delu uporabljajo informacijsko podporo.

3. faza – PREVERI – Spremljanje in pregled SUVI
Z načrtovanjem kontrol in kontrolnega okolja SUVI je potrebno začeti že v prvi fazi vzpostavitve sistema. Poleg tega je potrebno skozi celotno strukturo dokumentov, ki obravnavajo varovanje informacij, definirati kontrole in kontrolno okolje za nadzor nad

delovanjem SUVI. Skozi proces informiranja in usposabljanja je potrebno vse zaposlene s temi kontrolami seznanjati. Poleg tega je potrebno določiti postopke in odgovorne osebe za izvajanje teh kontrol, kakor tudi nadzor nad delovanjem teh oseb.

Vzpostavitev sistema kontrol in nadzora nad delovanjem SUVI v organizaciji vključuje naslednje aktivnosti:

- vzpostavitev kontrol in kontrolnega okolja,
- izvajanje kontrol in nadzora,
- nadzor nad delovanjem kontrol.

4. faza – UKREPAJ – Vzdrževanje in izboljševanje SUVI
Zadnja faza vzpostavitve SUVI v organizaciji je analiza odstopanj in izvajanje korektivnih in preventivnih ukrepov. Analiza odstopanj lahko pokaže, da udeleženci v poslovnih procesih organizacije niso ustrezno seznanjeni z zahtevami SUVI oziroma jih ne razumejo ali se ne zavedajo resnosti posledic njihovega nespoštovanja. V tem primeru je potrebno zagotoviti dodatno usposabljanje ali ustreznejši način informiranja. V kolikor analize pokažejo, da je potrebno določila v posameznih dokumentih SUVI spremeniti, mora biti določen postopek za izvedbo teh sprememb.

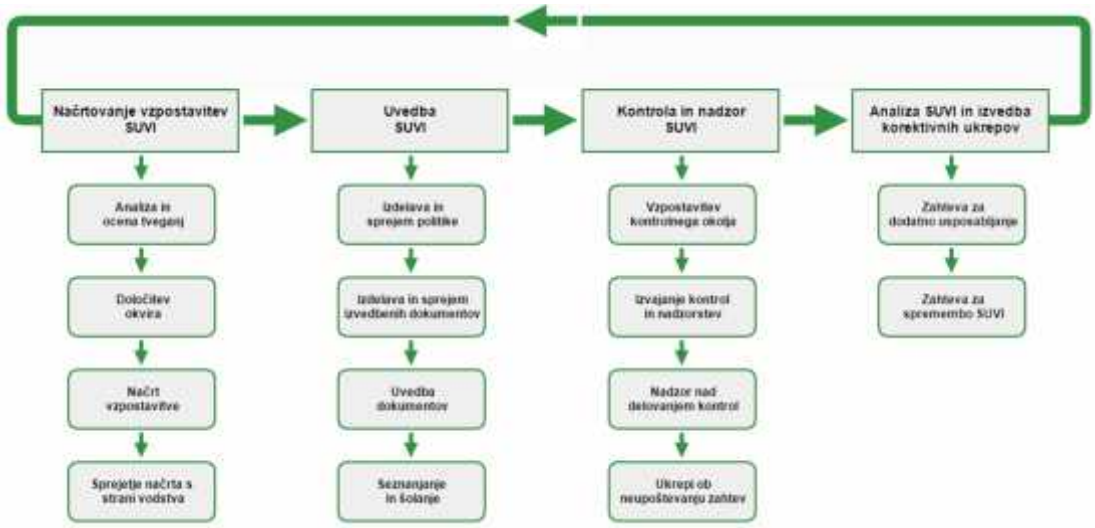
Aktivnosti zadnje faze vzpostavitve SUVI so:

- ugotavljanje učinkovitosti SUVI,
- po potrebi organiziranje dodatnega usposabljanja in izobraževanja,
- po potrebi uvajanje sprememb SUVI.

Zaradi tesne povezanosti informacij, informacijske tehnologije in poslovnih procesov lahko zaključimo, da tak način delovanja prinaša tudi nove zahteve za varno, zanesljivo in dolgoročno uspešno poslovanje.

Z vse večjim razvojem elektronskih komunikacij je postala varnost informacijskih sistemov ključnega pomena za zagotavljanje varnosti podatkov in informacij in eden glavnih dejavnikov pri izvajanju dejavnosti bank. Tega poslanstva pa ne moremo izpolnjevati brez izpolnitve nekaterih osnovnih pogojev ter celovitega pristopa. Kot je bilo že omenjeno, z varovanjem informacij ohranjamo zaupnost, celovitost in razpoložljivost.

Tako lahko zaključimo, da dosegamo varovanje informacij z določitvijo in vpeljavo ustreznih kontrol, ki ustrezajo varnostnim ciljem banke.



Slika 4: Model vzpostavitve SUVI v organizaciji (Brezavšček in Moškon 2010)

Omenimo lahko ključne razloge za uvedbo SUVI v bankah, in sicer:

- izboljšanje učinkovitosti upravljanja in varovanja informacij,
- skladnost z zakonodajo,
- dvig nivoja upravljanja z varovanjem informacij v banki,
- zmanjševanje poslovnih in operativnih tveganj v banki,
- zavedanje in odgovornosti zaposlenih glede varovanja informacij,
- dopolnjevanje z drugimi ISO standardi.

Poleg tega lahko omenimo, kot navaja možnost Skukan (1998), da bi se podjetja lahko ozko usmerila na točno določeno področje delovanja, ostale funkcije pa bi lahko prepustila za to specializiranim podjetjem, oziroma bi oddala delo v zunanje izvajanje (angl. *outsourcing*), kamor seveda lahko uvrstimo tudi računalništvo v oblaku. Prav zaradi čedalje večje uporabe oblačnih storitev v bančništvu v nadaljevanju navajamo trenutno veljavne regulatorne zahteve in priporočila politike uporabe zunanjih izvajalcev.

I. Uporaba zunanjih izvajalcev del

Republika Slovenija je dne 30.11.2015 izdala »Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice« (Uradni list RS, št. 73/15 in 49/16) (v nadaljevanju Sklep), kjer v četrtem odstavku 29. člena (politika uporabe zunanjih izvajalcev) med drugim določa, da mora banka zagotoviti, da so obveznosti in pravice, ki izhajajo iz pogodbe med banko in zunanjimi izvajalci, natančno opredeljene.
Zelo pomembno je vedeti, da morajo pogodbene pravice banke vključevati možnost predčasne prekinitve pogodbenega razmerja z zunanjimi izvajalci na zahtevo banke.

Poleg pogodbenih pravic banke pa so v tem členu določene tudi pogodbene obveznosti zunanjih izvajalcev, ki morajo vključevati:

- ustrezno zaščito podatkov banke,
- skladnost delovanja zunanjih izvajalcev s predpisi in standardi,
- popoln dostop pooblaščenih oseb ali funkcij banke do vseh prostorov in podatkov zunanjih izvajalcev, ki so povezani z opravljanjem zadevnih dejavnosti ter
- pravico do pregleda teh prostorov in podatkov.

Člen poleg navedenega poudarja nujnost določitve kvantitativnih in/ali kvalitativnih meril, saj lahko banka in zunanji izvajalec le na ta način ocenita ustreznost kakovosti storitev.

Sklep dodatno v drugem odstavku 29. člena določa, da mora banka zagotoviti, da uporaba zunanjih izvajalcev ne oslabi:
- izvajanja njenih poslovnih dejavnosti,
- obvladovanja tveganj iz prvega odstavka 23. člena tega sklepa in
- mehanizmov notranjih kontrol iz prvega odstavka 31. člena tega sklepa.

Preden banke začnejo z izločanjem pomembnega dela informacijskega sistema v zunanje izvajanje, se od njih pričakuje, da opravijo ustrezen skrbni pregled ponudnika (v okviru študije izvedljivosti) in izdelajo oceno izpostavljenosti tveganjem oziroma analizo tveganj.

Banke so poleg v tem poglavju že omenjenih zahtev dolžne natančno upoštevati tudi zahteve podane v obliki EBA smernic za oddajo del v zunanje izvajanje (angl. *Guidelines for Outsourcing*), ki so dostopne na spletni povezavi *http://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing*.

II. Opravljanje nadzora banke

Zakon o bančništvu (ZBan-2) v 242. členu (pregled poslovanja) določa, da mora banka omogočiti pooblaščeni osebi Banke Slovenije, da v skladu z zahtevo iz 243. člena tega zakona opravi pregled poslovanja banke na sedežu banke in v drugih prostorih, v katerih banka oziroma druga oseba po njenem pooblastilu opravlja dejavnosti in posle, v zvezi s katerimi Banka Slovenije opravlja nadzor.

III. Varovanje osebnih podatkov

Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1), stran 12707 v 53. členu (pristojnosti nadzornika) določa, da je pri opravljanju inšpekcijskega nadzora nadzornik upravičen pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter iznos osebnih podatkov v tretjo državo in posredovanje tujim uporabnikom osebnih podatkov.

IV. Zagotavljanje interne skladnosti poslovanja

Nenazadnje ne smemo pozabiti, da mora banka poleg navedenih regulatornih zahtev upoštevati tudi sprejete interne akte (npr. politiko upravljanja zunanjih izvajalcev, varnostno politiko, politiko upravljanja operativnih tveganj).

3.3. PSIHOLOŠKI VIDIKI VARNOSTI V VIRTUALNEM PROSTORU

Kot smo že omenili, je varnost informacijskega sistema postopek zaščite in zavarovanja računalniške in programske opreme, prav tako pa tudi podatkov, raznih fizičnih naprav, omrežij in osebja, pred nesrečami, namerno škodo ali naravnimi nesrečami. To mora biti neprekinjena dejavnost, ki traja 24 ur dnevno vse dni v letu.

Vodstvo podjetja je odgovorno za postavitev temeljne varnostne politike, zato mora razumeti, kaj in zakaj ščiti, ter seveda tudi pred kom. Vodstvo mora določiti tudi koliko sredstev je potrebno vložiti v varnostne ukrepe, ukrepi pa morajo biti široko zastavljeni, saj ni možno vedno vnaprej predvideti, od kod bo prišel napad. Za zagotavljanje varnosti je potreben sklop administrativnih, proceduralnih in tehničnih ukrepov.

Kontrole vodstva morajo temeljiti na treh principih (Gril, 2003, str. 6):
- posameznikovi odgovornosti,
- ločevanju nalog in
- nadzoru.

Kljub številnim drugim grožnjam je varovanje informacij pred osebjem zelo pomembno področje varovanja informacij, saj so lahko zaposleni ali drugi posamezniki za računalniški sistem zelo velika nevarnost, kar pomeni, da ga lahko ogrozijo na različne načine. Bratuša (2006) omenja, da so raziskovalci Univerze v Marylandu z uporabo konceptov klasične šole kriminologije želeli dokazati, da so ljudje resnično najšibkejši člen v povezavi s kibernetsko kriminaliteto in navajajo: »da je uporaba ugotovitev kriminologije pomembna pri preučevanju kibernetske kriminalitete, saj bi lahko pripomogli k razvoju konkretnih varnostnih politik, ki se ne bi osredotočale zgolj na tehnični vidik kibernetske kriminalitete, temveč tudi na človeško komponento.«

Naj omenimo, da se določeni podatki oziroma informacije lahko poškodujejo ali uničijo zaradi tega, ker zaposleni in drugi vpleteni niso izučeni ali pa so nevešči uporabe, torej ogrozijo informacije nenamerno. Zaposleni o različnih postopkih in izvedbah določenih procesov niso izučeni, jih ne poznajo ali pa o njih niso pravočasno obveščeni. V tem primeru lahko rečemo, da prihaja do uhajanja informacij in drugih pomembnih podatkov tudi zaradi slabega opolnomočenja zaposlenih. Opolnomočenje zaposlenih (angl. *employee empowerment*) je proces nudenja znanja, informacij in veščin zaposlenim, ki omogoča, da zaposleni sprejemajo avtonomne odločitve in zanje tudi odgovarjajo. Opolnomočenje sta Conger in Kanungo (1988, str. 472-479) predstavila z dveh vidikov, in sicer opolnomočenje kot dejavnik medsebojnih odnosov ter opolnomočenje kot motivacijski dejavnik. Tudi Geroy, Wright in Anderson (1998, str. 57) poudarjajo, da je opolnomočenje zaposlenih proces, kjer vodje zaposlenim nudijo potrebno usmerjanje ter veščine, ker jim je s tem omogočena avtonomija pri sprejemanju odločitev, hkrati pa odgovornost za odločitve nosijo zaposleni sami.

Daft in Noe (2001, str. 217) omenjata štiri elemente opolnomočenja zaradi katerih zaposleni svobodneje in odgovorneje izpolnjujejo delovne naloge:

- *informacije*: zaposleni imajo dostop do vseh informacij, vključno z informacijami o uspešnosti podjetja ter osebnih dohodkih vrhnjega managementa;
- *znanje*: organizacije zaposlenim nudijo izobraževalne programe oz. usposabljanje, ki jim pomaga osvojiti znanje ter veščine, ki so potrebne za opravljanje določenega dela ter doprinos k uspešnosti poslovanja organizacije;
- *moč*: zaposlenim je potrebno dati možnost oz. moč za samostojno odločanje. Z uporabo krožkov kakovosti ter samousmerjajočih se timov lahko zaposleni vplivajo na delovne procese in uspešno delovanje organizacije;
- *nagrada*: zaposleni so nagrajeni glede na uspešnost celotne organizacije.

Znanje in informacije so vsekakor bistvenega pomena za kvalitetno izvedbo delovnih nalog. Informacije morajo glede produktivnosti dela, strategije, ciljev in konkurenčnosti postati bolj dostopne večjemu številu zaposlenih na različnih ravneh organizacije in na več načinov, kot so bile do uvedbe opolnomočenja. Le na ta način lahko zaposleni bolje razumejo, kako s svojim delom omogočajo podjetju zasledovanje ciljev (Spreitzer, 1996, str. 488).

Tudi Wickisier (1997, str. 215) opozarja, da je potrebno zaposlene izobraževati o sprejemanju odločitev, reševanju konfliktov, vodenju ter racionalni porabi sredstev, saj večinoma nimajo izkušenj z opolnomočenjem.

Opolnomočenje Lee & Koh, (2001, str. 686) definirata tudi kot kombinacijo psihološkega stanja zaposlenih, na katere vplivajo tudi opolnomočenjska vedenja vodij. Kaplan (1991, str. 9) omenja, da se veliko zaposlenih težko prilagaja na spremembe zaradi lastnih vedenjskih vzorcev. Zaposlene je potrebno z različnimi interventnimi pristopi informirati, poučiti in jih ozavestiti, da spremenijo določene vedenjske vzorce oziroma, da opustijo stare navade ter sprejmejo nov način vedenja (Demšar Pečak, 2014). Zato je zelo pomembno, da v organizacijah zaposlenim ves čas nudijo različna izobraževanja, tehnično podporo in pomoč, še prav posebej pa morajo biti pozorni na njihovo psihično stanje oziroma duševno zdravje. V prihodnjih poglavjih bomo model opolnomočenja zaposlenih pri varni uporabi oblačnih storitev v bančništvu natančneje opredelili.

V nadaljevanju navajamo nekaj definicij oz. razmišljanj o duševnem zdravju. Biti duševno zdrav, kot omenja Konec Juričič (b. d.), »… ne pomeni zgolj ne imeti takšne ali drugačne duševne motnje, saj duševno zdravje poenostavljeno lahko opišemo še z najmanj tremi drugimi merili. Prvo merilo opredeljuje človekovo notranje psihično stanje: sreča, dobro počutje, zadovoljstvo s samim seboj, dobra podoba o sebi. Drugo merilo duševnega zdravja so človekovi odnosi z drugimi in njegovo delovanje: dobri odnosi z ljudmi okoli nas, razumevanje drugačnosti, uspehi pri delu v šoli, službi in drugih dejavnostih, ki jih opravljamo. Tretje merilo duševnega zdravja je sposobnost človeka, da obvladuje svoje življenje in se uspešno sooča z različnimi situacijami, nalogami, obremenitvami in težavami«. Zato lahko rečemo, da kvaliteta medosebnih

odnosov zelo vpliva na posameznikovo telesno in duševno zdravje, stres pa ima ključno vlogo pri nastanku somatskih in emocionalnih motenj, saj deluje na celotno biopsihosocialno naravo človeka (Demšar Pečak, 2014).

Omeniti pa je potrebno, da se lahko zgodi, da zaradi prevelike obremenjenosti in stresa na delovnem mestu pri zaposlenih pride do različnih psihosomatskih obolenj in drugih psihičnih motenj, kar ima za posledico neustrezno, nenatančno, slabo opravljeno delo, deviantno vedenje ali pa celo kriminalna ravnanja. Preučevanje stresa se je začelo v petdesetih letih, ko je pojem »stres« prvi uvedel zdravnik Hans Selye (1950) in opisal model stresa ter njegove posledice kot »splošni adaptacijski sindrom« (ang. *General Adaptation Syndrome*). Stres lahko tudi označujemo kot »program telesnega prilagajanja novim okoliščinam, njegov odgovor na dražljaje okolja, kot psihosomatski mehanizem za uravnavanje in uravnoteženje napetosti, kar enostavno povedano pomeni, zaznavo in pripravo telesa na posamezne obremenitve« Schmidt (2003, str. 7).

Kar je za nekoga negativni stres, je lahko za nekoga drugega izziv ali celo motivator, zato ga lahko opredelimo kot neskladje med določenimi zahtevami in posameznikovimi sposobnostmi. Lahko rečemo, da je stres posledica neravnovesja med zahtevami okolja in lastno usposobljenostjo. Če med njimi ne zmoremo vzpostaviti ravnotežja, pride do negativnega doživljanja stresa, na katerega se začne obrambno odzivanje, ki je nehotno, avtomatično in varuje osebno integriteto (Lamovec, 1998; Schmidt, 2003). Prav zato moramo, kot navaja Demšar Pečak (2014), razumeti tudi psihološko plat posameznika in dejavnike, ki vplivajo na proces njegovega odločanja. Ni dovolj, da smo seznanjeni z vrednotami in stališči, ki jih ima posameznik, moramo jih tudi razumeti in poznati.

Razne psihične motnje se lahko odražajo tudi v duševnem zdravju posameznika, neustreznih medosebnih odnosih med samimi zaposlenimi, kot tudi v odnosu do zunanjih sodelavcev. V nadaljevanju bomo opredelili različne motnje, ki lahko privedejo do deviantnega vedenja posameznikov. Osebnostne motnje priročnik DSM-IV-TR (Erzar, 2007) opredeljuje kot »trajne vzorce dojemanja, komuniciranja in razmišljanja o sebi, drugih in svetu, ki se kažejo v najrazličnejših socialnih in medosebnih situacijah«.

Odnos med stresom in zmogljivostjo zaposlenih je grafično prikazan na sliki 5 (Beales, Nunn, 2011; povzeto po Inštitutu za produktivnost (2016)):

Slika 5: Odnos med stresom in zmogljivostjo zaposlenih (Beales, Nunn, 2011; povzeto po Inštitutu za produktivnost (2016)

Psihološke teorije se v celoti osredotočajo na posameznika, in sicer na psihološke dejavnike, ki vplivajo na razvoj deviantnega vedenja. Glede na posebnosti kibernetskega prostora psihološki dejavniki nedvomno odigrajo pomembno vlogo pri izvedbi kaznivega dejanja v kibernetskem prostoru. Prestopniško vedenje je lahko obravnavano tudi z vidika duševnih deviacij posameznika (Bratuša, 2006). Psihopatologijo bi lahko opredelili tudi kot »obseg znanja o motnjah duševnega (psihičnega) delovanja možganov« (Kobal, 2009 str. 15), omeniti pa je potrebno še, da patologija nima zgolj biološke in psihološke podlage, ampak je prisoten še vpliv družbenih dejavnikov na posameznika (Meško, 1998; str. 160-161).

Bratuša (2006) še omenja, da strokovnjaki v povezavi z osebnostnimi motnjami trdijo, da obstajajo nekatere osebnostne karakteristike, ki napovedujejo verjetnost kaznivih dejanj. Ob obravnavi osebnostnih motenj, kot je treba poudariti, ne moremo avtomatično povezovati nagnjenosti z deviantnostjo, kljub temu pa izražajo potencialno večjo nagnjenost posamezniki z antisocialno, narcistično in mejno osebnostjo. Kot smo že omenili, lahko pri obravnavi storilcev kibernetske kriminalitete še posebej izpostavimo *antisocialno osebnostno motnjo*, katere ključna lastnost je nespoštovanje in kršenje pravic drugih. Ljudje z antisocialno osebnostno motnjo so neodgovorni, neiskreni, impulzivni, prevarantski in lažnivi (Erzar, 2007). Omenimo lahko tudi *mejno osebnostno motnjo.* V tem primeru gre za dolgotrajno motnjo v osebnostnem delovanju, za katero je značilna intenzivna čustvena nestabilnost, ki vpliva na predstavo posameznikove identitete, vzpostavljanje odnosov z drugimi ljudmi in njegovo vedenje. Posamezniki s takšno motnjo so problematični zaradi svoje impulzivnosti in tveganega vedenja (npr. tvegane vožnje, spolnosti, popivanja, drogiranja), imajo težave pri nadzoru čustev in impulzov ter intenzivne kratke epizode anksioznosti in depresije (Inštitut za razvoj človeških virov, 2016). Kot tretjo osebnostno motnjo lahko omenimo *narcistično.* Za osebe s to motnjo je značilen razcep v samopodobi, in sicer na zunanjo, idealno in

grandiozno podobo, ter notranjo, razvrednoteno krhko in ranljivo podobo, pri čemer je ključni namen zunanje samopodobe ščitenje krhke notranje samopodobe pred občutkom razvrednotenja. Posamezniki s takšno motnjo v ospredju vidijo zgolj sebe, medtem ko so do drugih brezbrižni in izkoriščevalski, hkrati pa izkazujejo pomanjkanje empatije (Inštitut za razvoj človeških virov, 2016).

Šket (2009) omenja, da posamezniki, ki niso zadovoljni s svojim življenjem, pogosto prilagodijo svojo identiteto v virtualnem okolju. To se lahko kaže kot sprememba spola, starosti, izobrazbe ali naziva, saj je posameznik v virtualnem okolju varno skrit za svojim ekranom, zato dobi občutek nevidnosti, kar pa nekoliko spodbuja oz. omogoča posameznikom aktivnosti, v katere se drugače morda ne bi vključili. Virtualno okolje zabriše mejo med resničnim in fantazijskim, zato posamezniki nelegalnih in nasilnih dejanj ne dojemajo enako kot v fizičnem okolju. Poleg tega se virtualni vidik uporablja tudi kot opravičilo za izvajanje dejanj, pri čemer gre za nezavedno uporabo obrambnih mehanizmov storilca.

Lahko pa se zgodi, da posamezniki poškodujejo ali uničijo podatke *namerno***,** na primer s kršenjem pravil in zakonov in izrabljajo sistem v svojo korist. Nenazadnje pa lahko omenimo tudi kriminalce oz. kriminalne skupine, ki z informacijami trgujejo in jih zlorabljajo.

Te dejavnosti so, kot navaja Bratuša (2006, str. 316), odvisne od naslednjih dejavnikov:

- *možnost dostopa*: obseg škode v določenem sistemu je odvisen od omejenosti vstopa v računalnik oz. sistem in od tega, do katere meje ima oseba avtorizacijo za vstop v sistem. Upoštevati je potrebno tudi, ali ima uporabnik dostop do glavnega računalnika ali samo do terminala ter ali ima dostop do programske opreme oz. dela v sistemu;
- *stopnja znanja*: z uporabnikovim velikim obsegom znanja se možnost namernega ogrožanja veča, hkrati pa sta lahko prav neznanje in ignoranca še veliko večja nevarnost;
- *motivacija*: največja nevarnost na tem področju so nedvomno tisti zaposleni, ki imajo neposreden dostop v določen sistem. Omeniti je potrebno, da tveganje lahko zmanjšamo na tak način, da preverjamo njihovo preteklost, drugi način je njihovo učinkovito nadzorovanje, tretji pa usposabljanje in krepitev občutka odgovornosti. Najbolj nevarni pa so sami vzdrževalci računalniške opreme, saj najbolj poznajo sistem, ki ga vzdržujejo in ki so ga tudi namestili.

Posebej pa je potrebno omeniti profesionalne vsiljivce ali hekerje, proti katerim pa se je nemogoče popolnoma zavarovati, saj svoje vdore sproti prilagajajo in vedno znova odkrivajo pomanjkljivosti v programski oziroma strojni opremi. Termina »heker« in »hekanje« izvirata iz angleškega izraza »*to hack away at something until it gives way*«, kar pomeni, da neko stvar toliko časa krhaš, da se na koncu vda oz. da v sistemu odkriješ slabost, ki jo lahko izkoristiš. Izraz so začeli uporabljati ameriški študentje kot oznako za prebrisane bližnjice pri programiranju s poudarkom na spretnosti manipulacije z informacijsko komunikacijsko tehnologijo (Britz v Bratuša, 2006). Rogers (v Bratuša, 2006) hekerje razvrsti v več skupin, in sicer na: novince, kiber-huligane, koderje

virusov, malenkostne tatove, hekerje stare šole, profesionalne kriminalce in notranje osebje. Slednje bomo natančneje opredelili v nadaljevanju.

Kot smo že omenili, notranje osebje, torej zaposleni, predstavljajo največje tveganje in lahko povzročijo največ škode, kljub temu pa se jih najpogosteje zanemarja kot varnostno grožnjo. Največkrat so to nezadovoljni zaposleni ali pa nekdanji zaposleni, njihov motiv je najpogosteje maščevanje zaradi domnevnih krivic. Takšne osebe imajo precejšnje znanje o delovanju organizacije, pogosto imajo tudi visoko stopnjo dostopa do občutljivih sistemov in podatkov. Najpogosteje so zaposleni na področju informacijsko komunikacijskih tehnologij in zato dosegajo nezanemarljivo stopnjo tehnične usposobljenosti (Bratuša, 2006).

Občutljive informacije in podatke lahko pred zaposlenimi in drugimi osebami (npr. vzdrževalci) zavarujemo z različnimi ukrepi, kot na primer z natančnim pregledom preteklih aktivnosti oziroma zaposlitev bodočega novo zaposlenega, preveriti je tudi potrebno pogodbe z oskrbovalci sistema in ugotoviti, ali oni preverjajo preteklost svojih zaposlenih. Poleg tega pa je za varnost potrebno usposobiti zaposlene za prepoznavanje sumljivih dejavnosti ter poročanje o njih in ustrezno usposobiti še nadzorno osebje. Potrebno je omeniti, da morajo biti navodila in postopki za uporabo sistema in programov natančno določena, hkrati pa je potrebno zaposlenim, ko zapustijo podjetje, onemogočiti dostop do sistema ter od njih zahtevati vrnitev vseh ključev, magnetnih kartic in podobno.

4. ANALIZA ODMEVNIH PRIMEROV ZLORAB V OBLAČNIH STORITVAH

4.1. ZLORABE, KI SO PRIZADELE POSAMEZNIKE

Kot smo že omenili, avtorji navajajo (Bratuša, 2006; Dimc & Dobovšek, 2012; Gradišar etal., 2005), da o računalniški kriminaliteti govorimo v primerih, pri katerih je uporaba računalniške opreme bistvena pri izvedbi kaznivih dejanj, vendar pa je potrebno omeniti, da je termin kriminaliteta povezan z računalnikom, ki ne igra nujno ključne vloge, saj je lahko uporabljen zgolj kot pripomoček.

Omeniti je potrebno, da se razsežnosti, ki jih prinaša kibernetski prostor, izražajo na karakteristikah kibernetske kriminalitete, zato je zelo privlačna za moderne kriminalce in kriminalne organizacije. Ključne karakteristike so: neosebni vidik, mednarodne razsežnosti, mehanski vidik ter tako imenovano ogrinjalo anonimnosti (Chantler, 1996). Kombinacija naštetih značilnosti potencira virtualno videnje kibernetske kriminalitete pri storilcih in pogosto tudi pri splošni javnosti. Različne zlorabe oblačnih storitev lahko prizadenejo tako posameznike kot tudi organizacije.

Kot primer zlorab oblačnih storitev, ki so prizadele posameznike, lahko omenimo kanadsko spletno stran Ashley Madison, ki šteje 37 milijonov članov, ki jo uporabljajo posamezniki, da lažje diskretno varajo svoje partnerje. Leta 2015 je bila omenjena spletna stran žrtev vdora neznanih napadalcev. Ti so ukradli vse podatke o uporabnikih in jih začeli objavljati na internetu. Grozili so, da bodo razkrili celotno podatkovno bazo s podatki o naslovih in plačilih uporabnikov skupaj z njihovimi spolnimi fantazijami, če spletne strani ne bodo ukinili (Huš, 2015). Zaradi razkritja omenjenih podatkov (Crnovič, 2015) je iz obupa prišlo do dveh samomorov in več primerov izsiljevanja. Matična družba Ashley Madison, Avid Life Media, je za informacije, ki bi pripeljale do prijetja hekerjev, ponudila pol milijona kanadskih dolarjev oziroma 327 tisoč evrov.

4.2. ZLORABE, KI SO PRIZADELE ORGANIZACIJE

Različne zlorabe oblačnih storitev lahko prizadenejo tudi organizacije. Omenimo lahko kar nekaj primerov.

Eden izmed najslavnejših hekerjev, Kevin Mitnick, je med drugim izvedel vdore v najrazličnejše sisteme (Nokia, Motorola, NEC, Sun Microsystems, Fujitsu Siemens, itd.) z uporabo tehničnih veščin v kombinaciji s socialnim inženiringom. Mitnick je bil zaprt kar dvakrat, in sicer prvič leta 1988 in drugič leta 1995, ko je dobil petletno zaporno kazen. Leta 2000 je bil pogojno izpuščen, vendar do izteka pogojne kazni leta 2003 ni smel uporabljati interneta. Mitnick je bil uspešen predvsem zaradi svojih sposobnosti kot socialni inženir in je s tega področja napisal tudi nekaj knjig. Danes ima svoje podjetje, ki se ukvarja z informacijsko varnostjo (Silverman, 2012).

Prav tako lahko omenimo t.i. »brezdomnega hekerja«, Adriana Lamoja, znanega po tem, ker je občasno živel v zapuščenih stavbah in izvajal hekerske dejavnosti v knjižnicah in cyber-kavarnah. Lamo je izvedel vdore v več pomembnejših organizacij (Microsoft, New York Times, Yahoo, Google, itd.), pri katerih je šlo vedno za penetracijske teste. S podjetji je zatem vzpostavil stik in jih obvestil o njihovi ranljivosti. Lamo je bil obsojen na šest mesecev pripora in dvoletno pogojno kazen. Leta 2010 mu je bil diagnosticiran Aspergerjev sindrom, zaradi česar je bil tudi hospitaliziran. Leta 2011 se je ponovno pojavil v novicah zaradi prijave Bradleya Manninga, ki naj bi predajal zaupne dokumente organizaciji Wikileaks, kar je hekerska skupnost ostro obsodila in označila Lamoja kot izdajalca (IT Security Editors, 2012; Dimc & Dobovšek, 2012).

Različni avtorji omenjajo Kevina Poulsna, bolj znanega po vzdevku Dark Dante, ki je začel s hekanjem pri 17 letih. Znan je postal po vdoru v telefonsko centralo radia KIIS-FM, kjer je prevzel nadzor nad vsemi telefonskimi linijami in si s tem pridobil glavno nagrado – avtomobil znamke Porsche. Po aretaciji je priznal kazniva dejanja, kot so najrazličnejše goljufije, pranje denarja ter vdor v sistem FBI, kjer je imel dostop do tajnih podatkov. Poulsen je bil obsojen na 51 mesecev zaporne kazni in denarno kazen v višini 56.000 dolarjev. Po prestani zaporni kazni se je zaposlil kot novinar in je urednik Wired News. Kot zadnji primer lahko omenimo še Jonathana Jamesa, znanega po vzdevku »Comrade«, ki je bil prvi obsojen mladoletni heker. Izvedel je vdore v različne sisteme (npr. Bell South, Defense Thread Reduction Agency, NASA, itd.), za kar je dobil šest mesecev zapora. V letu 2008 je bil ponovno obdolžen sodelovanja pri eni največjih kraj identitet v ameriški zgodovini, in sicer naj bi bili ukradeni podatki o kreditnih karticah več kot milijon strank verige trgovin TJX podjetja DSW, OfficeMax, itd. Dva tedna po obdolžitvi je naredil samomor (Dimc & Dobovšek, 2012; Silverman, 2012).

Na podlagi omenjenih primerov lahko zaključimo, da pravzaprav absolutno varen sistema nikoli ne bo obstajal, saj je, kot omenja Vidmar (2011), stopnja varnosti odvisna predvsem od nevarnosti, ki sistemu in uporabnikom objektivno grozijo.

4.3. DELOVANJE POSAMEZNIKOV IN SKUPIN, KI SO POVZROČILE VARNOSTNE INCIDENTE

Kibernetske kriminalce lahko razvrstimo na podlagi prilagojenega FBI profila MICE, ki je kratica izpeljana iz angleških besed »*money*« oz. denar, »*ideology*« oz. ideologija, »*compromise*« oz. kompromis in »ego« (Radcliff v Bratuša, 2006). Velikokrat se zgodi, da hekerji vstopajo v prepovedan kibernetski prostor zaradi različnih ideologij, političnih prepričanj, družbeno-kulturnih vplivov, verskega prepričanja in drugih vzrokov.

V primerih, kjer je ideologija ključni motiv za izvedbo dejanja kibernetske kriminalitete, gre najpogosteje, kot navaja Bratuša (2006), za hektivizem in tudi kibernetski terorizem, saj se v teh primerih izvajajo najrazličnejša dejanja, s katerimi se poskuša onemogočiti

ali škodovati targetirani organizaciji ali državi, na primer z razobličenjem spletnih strani, z napadi, ki onemogočajo storitve, vdori v sisteme, itd.

Kot primer posameznikov lahko omenimo avstralskega političnega aktivista, raziskovalnega novinarja, bivšega računalniškega hekerja, programerja in tiskovnega predstavnika WikiLeaksa, Juliana Paula Assangea (WikiLeaks je mednarodna neprofitna medijska organizacija, ki v okviru spletnega portala, zgrajenega s tehnologijo wiki, objavlja tajne oziroma širšim množicam nedostopne dokumente, prejete s strani anonimnih virov). Julian Paul Assange je leta 2010 javno objavil videoposnetek helikopterja Združenih držav Amerike, kako strelja na civiliste in novinarje Reutersa v Iraku (Krečič, 2013). Bradley (Chelsea) Manning, ki je razkril ta dokument, je bil obsojen na 35 let zapora, medtem ko proti strelcu oziroma pilotu in njunemu nadrejenemu niso uvedli nobenih disciplinskih postopkov. Ti še vedno služijo v ameriški vojski. Chelsea Manning je trans ženska in ko je bilo njeno ravnanje razkrito, je bila znana kot moški Bradley Manning, ki je bil zaprt že več kot pet let (Amnesty Inetrnational, 2015).

Naslednji je Edward Joseph Snowden, ameriški obveščevalec ali žvižgač. Izraz žvižgači izhaja iz angleške besede *whistleblower*. To so zaposleni ali bivši zaposleni posameznih organizacij, ki opozarjajo na nezakonitosti, nepravilnosti ali dejanja, ki ogrožajo javno varnost ali zdravje. Razkrivajo različne kršitve, domnevno nepošteno, neetično, neprimerno ali nelegalno in diskriminatorno dejavnost, ki se pojavlja v organizaciji in jo izvajajo sedanji ali nekdanji zaposleni oz. člani (Merljak, 2013). Edward Joseph Snowden, nekdanji pogodbeni sodelavec ameriške nacionalne varnostne agencije NSA, je junija leta 2013 razkril informacije o ameriškem nadzorovanju telefonskih in spletnih informacij v ZDA in tujini. Objavil je različne strogo zaupne dokumente programov NSA.

V prepovedani kibernetski prostor pa hekerji vstopajo tudi zaradi denarja, ki danes predstavlja najpogostejši motiv vseh tipov storilcev kibernetskega kriminala, od najbolj usposobljenih hekerjev pa do prevarantov z nizko stopnjo tehničnega znanja.

Kot primer skupine, ki je povzročila varnostni incident, lahko omenimo Projekt Panama Papers. Avtorji Obermayeret al. (2016) navajajo, da je projekt nastal na temelju notranjih podatkov malo znane a vplivne odvetniške družbe Mossack Fonseca s sedežem v Panami ter podružnicami v Hongkongu, Miamiju, Zürichu in več kakor 35 drugih krajih po svetu, ki jih je od anonimnega vira pridobil nemški časnik Süddeutsche Zeitung. Pri tem je sodelovalo 376 novinarjev iz 76 držav. Družba je ena najuspešnejših svetovnih ustanoviteljic navideznih družb v davčnih oazah, torej oblike podjetniškega poslovanja, s katerim je mogoče prikriti lastništvo premoženja. Razkriti notranji dokumenti odvetniške družbe vsebujejo informacije o 214.488 poslovnih subjektih s sedežem v tujini, ki so povezani z ljudmi v več kakor 200 državah in ozemljih. Med podatki so elektronska sporočila, finančne preglednice, potni listi in dokumenti o poslovanju podjetij, ki razkrivajo skrivne lastnike bančnih računov in podjetij na 21 sodnih območjih v davčnih oazah, od Nevade do Singapurja in Britanskih Deviških otokov. Skrivni dokumenti kažejo, da je odvetniška družba tesno sodelovala z velikimi

bankami in velikimi odvetniškimi družbami na Nizozemskem, v Mehiki, Združenih državah Amerike in Švici ter pomagala strankam prenašati denar ali zmanjšati njihove davčne odhodke. Veliko razkritje dokumentov omogoča vpogled v premoženje v davčnih oazah dvanajstih sedanjih in nekdanjih svetovnih voditeljev ter razkriva, kako so sodelavci ruskega predsednika Vladimirja Putina na skrivaj prenesli kar 2 milijardi dolarjev prek bank in skrivnih podjetij tako, da so prikrivali plačila in dokumente, datirane za nazaj, ter na skrivaj pridobivali vpliv v ruskih medijih in avtomobilski industriji.

Obermayer et al (2016) navajajo, da dokumenti odkrivajo tudi podrobnosti o skritih finančnih poslih 128 politikov in javnih uradnikov po svetu. Vsega skupaj kar 11,5 milijona dokumentov kaže, kako globalna industrija odvetniških družb in velikih bank prodaja finančno tajnost politikom, goljufom, trgovcem z mamili in terorističnim organizacijam pa tudi milijarderjem, znanim osebnostim in športnim zvezdnikom. Med razkritimi dokumenti so se tako znašli tudi:

- družina kitajskega državnega voditelja Xi Jinpinga, ki je podprl boj proti korupciji,
- ukrajinski predsednik Peter Porošenko, ki se predstavlja kot reformist v državi, ki jo pretresajo korupcijski škandali,
- poslovanje pokojnega očeta britanskega premiera Davida Camerona s podjetji s sedežem v tujini, njegov sin pa velja za voditelja, ki poskuša reformirati zakonodajo, ki ureja poslovanje z davčnimi oazami,
- islandski premier Sigmundur Davíð Gunnlaugsson in njegova žena, ki sta na skrivaj imela podjetje s sedežem v tujini, ki je med finančno krizo v državi hranilo na milijone dolarjev v islandskih bančnih obveznicah,
- Lionel Messi, najboljši nogometaš na svetu – z očetom sta bila lastnika panamske družbe Mega Star Enterprises Inc (njegovo poslovanje v davčnih oazah pa trenutno preiskujejo v Španiji, kjer preverjajo, ali je to bila utaja davkov ali ne),
- filmski zvezdnik Jackie Chan, lastnik vsaj šestih podjetij, ki jih upravlja odvetniška družba,
- obsojeni pralec denarja, ki je trdil, da je poskrbel za nezakonit prispevek, vreden 50.000 dolarjev, ki so ga izplačali vlomilcem v primeru Watergate,
- 29 milijarderjev, ki so navedeni na seznamu 500 najbogatejših ljudi na svetu revije Forbes,
- člani Fife - zveze, ki določa pravila v mednarodnem nogometu.

Družba Mossacka Fonsece je zatrdila strankam, da jim ni treba skrbeti, saj jim je zagotovila, da je zanjo zaščita zasebnosti strank »vedno na prvem mestu, zato so njihove zaupne informacije shranjene v tehnološko najnaprednejšem podatkovnem središču, vsakršno sporazumevanje v globalnem omrežju pa je obdelano s šifrirnim algoritmom, ki ustreza najvišjim svetovnim standardom«. Kot pa smo že omenili, absolutna varnost, kljub najvišjim standardom varnosti, nikoli ni mogoča.

Omenimo lahko še nekaj drugih primerov hekerskih skupin, in sicer skupino Masters of Deception, ki je bila odgovorna za najrazličnejša dejanja kibernetskega kriminala (kraja

zaupnih podatkov, vdori v sisteme, kraja kreditnih kartic, itd.). Skupino so ustanovili hekerji kot odgovor na takrat najbolj popularno hekersko skupino Legion of Doom, ki naj bi izgubila prvotni pomen, zaradi česar je slavni heker Mark Abene z vzdevkom Phiber Optik prestopil iz ene skupine v drugo. Skupina je med drugim objavljala Legion of Doom Technical Journals, ki so vsebovali nasvete in informacije o hekanju (Dimc & Dobovšek, 2012, str 147). Druga hektivistična skupina, znana po svojem napadu na Atomic Research Center v Indiji, se je imenovala Milworm. Njen namen je bilo poudarjanje protijedrskih prepričanj. Z napadom naj bi namreč posvarili svet pred nevarnostjo jedrskega orožja v rokah Indije in Pakistana. Omenjeni napad so izvedli najstniki, najmlajši član je bil star le 15 let (Dimc & Dobovšek, 2012, str. 148).

Na koncu lahko omenimo še Anonymous, kot eno izmed bolj odmevnih hekerskih oz. hektivističnih skupin zadnjega časa, saj zagovarja svoboden dostop do vseh vsebin na svetovnem spletu in nasprotuje cenzuri ter izvajanju nadzora nad dejavnostmi v virtualnem okolju. Poleg napada na Sonyjevo mrežo Playstation je skupina izvedla napade na najrazličnejše vladne in nevladne organizacije in njihove spletne strani. Gre za decentralizirano spletno skupnost, katere člani delujejo anonimno za doseganje dogovorjenih ciljev (Auza, 2011).

5. USPOSABLJANJE ZAPOSLENIH ZA VARNO UPORABO OBLAČNIH STORITEV

Izobraževanje in usposabljanje zaposlenih za varno uporabo oblačnih storitev je v organizacijah ključnega pomena. Pomembno je, da se izobraževanj udeležujejo vsi zaposleni v organizaciji, prav tako pa tudi poslovni partnerji. Izobraževanja se razlikujejo glede na to, komu so namenjena, saj gre lahko za usposabljanje vodstva, delavcev ali pa tudi ključnih uporabnikov informacijskih sredstev. Zaradi spreminjanja stvari, povezanih z informacijsko varnostjo, je ključnega pomena tudi, da se izobraževanja konstantno ponavljajo in dopolnjujejo. Taka izobraževanja lahko potekajo v obliki seminarjev ali delavnic, oziroma tudi seminarjev zaposlenih preko e-izobraževanja, torej interneta, kjer pridobivajo pomembna nova znanja o varnosti informacijskih sredstev. Med sicer različnimi metodami usposabljanja je vedno manj klasičnih oblik izobraževanja, saj sodobna informacijska tehnologija omogoča vpeljavo velikega števila novih učnih metod in učenje na daljavo, to pa omogočajo tehnološko podprta izobraževanja, uporaba interneta in reševanje konkretnih problemov. Različni programi usposabljanja so zelo pomembni, saj je za organizacijo pomembno, da zagotovi prenos znanja in izkušenj med zaposlenimi.

5.1. PRIMER DOBRE PRAKSE USPOSABLJANJA ZAPOSLENIH

Fabiani (2013) je v svoji raziskavi ugotovila, da oblačne storitve tudi v javni upravi prinašajo prednosti, kar se največkrat kaže v obliki prihrankov pri stroških ter večje učinkovitosti in fleksibilnosti. V javni upravi lahko govorimo o državnem oblaku oz. vladnem oblaku, ki pa ga opredeljujemo tudi kot celoto oblačnih storitev, ki jih ponuja javna uprava za svoje storitve (Catteddu & Hogben, 2012). Za posamezne organizacije je premik v oblačne storitve dokaj preprost, za javno upravo pa je vpeljava oblačnih storitev velik zalogaj. Craig et al, (2009) opozarja, da mora država, ki želi prenesti svoje poslovanje v oblak temeljito premisliti o vseh pričakovanih prednostih in tveganjih ter skrbno načtovati to odločitev.

Kot največjo oviro glede državnega oblaka avtorica omenja nenaklonjenost javne uprave spremembam, prav tako pa tudi neustrezne standarde v povezavi z varnostjo podatkov, saj kot vemo, oblačne storitve ne prinašajo samo prednosti, ampak tudi določena tveganja. Varnost podatkov je še toliko bolj pomemben dejavnik za javno upravo, saj pristojni državni organi shranjujejo in obdelujejo osebne podatke državljanov, zato lahko ob njihovi zlorabi pride do katastrofalnih posledic (Catteddu & Hogben, 2012, 5).

Omenimo lahko, da je slovenska vlada že leta 2008 začela pripravljati Strategijo učinkovite državne informatike, od februarja leta 2016 pa imamo v Sloveniji potrjen dokument z naslovom »Strategija kibernetske varnosti - vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti«.
Kot primer dobre prakse usposabljanja zaposlenih za varno uporabo oblačnih storitev navajamo »Priporočila informacijske varnostne politike javne uprave«, ki jih je na

podlagi 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07 in 31/08), dne 28.10.2010 izdalo Ministrstvo za javno upravo, z namenom zaščite informacijskega premoženja, ki ga upravlja javna uprava. V dokumentu je 167. členov, ki jih morajo upoštevati tako vodstvo, zaposleni kot tudi osebe pogodbenih izvajalcev oziroma vsi, ki imajo dostop do omenjenega informacijskega premoženja.

Usposabljanj na temo varovanja podatkov se morajo v obliki celodnevnih seminarjev udeleževati vsi zaposleni, ki so kakorkoli povezani z zaščito informacijskega premoženja. Primer gradiva usposabljanja je dostopen na spletni povezavi *http://www.uvtp.gov.si/si/delovna_podrocja/usposabljanje/osnovno_usposabljanje.*

V Priporočilih informacijske varnostne politike javne uprave so v 5 točkah strnjene naslednje politike:

1. politika fizičnega varovanja:
   - fizični dostop,
   - varovanje sredstev za dostop,
   - varovanje opreme,
2. politika primerne rabe informacijskih sistemov in zaščite občutljivih podatkov:
   - uporaba opreme informacijske tehnologije,
   - zlonamerna programska oprema,
   - informacijski sistemi,
   - upravljanje izmenljivih nosilcev podatkov,
   - dostop do informacijskih sistemov,
   - načelo čiste mize,
   - načelo praznega zaslona,
   - oddaljeni dostop,
   - pravice nad podatki elektronske pošte,
   - privzete nastavitve predala,
   - velikost elektronskih sporočil,
   - šifriranje in podpisovanje elektronskih sporočil,
   - brisanje elektronskih sporočil,
   - posebna pooblastila,
   - dostop do podatkov,
3. politika nabave opreme in storitev pri zunanjih izvajalcih:
   - priprava javnega naročila,
   - varnostni elementi v pogodbi,
   - nadzor
4. politika razvoja in vzdrževanja informacijskih sistemov in obvladovanja sprememb:
   - načrtovanje,
   - razvojno okolje,
   - testno okolje,
   - izobraževalno okolje,
   - produkcija
5. politika upravljanja informacijskega sistema:

- upravljanje produkcijskega okolja,
- dokumentirani delovni postopki,
- upravljanje sprememb v produkcijskem okolju in omrežju,
- ločevanje nalog,
- zaščita pred zlonamerno in prenosno kodo,
- časovna uskladitev,
- nadzor dostopa do omrežja,
- ločevanje v omrežjih,
- upravljanje omrežnega usmerjanja,
- upravljanje incidentov pri varovanju informacij,
- dnevniški zapisi,
- obdelava podatkov v dnevniških zapisih,
- ravnanje na podlagi ugotovitev iz dnevniških zapisov,
- kriptografske rešitve,
- raba virov,
- oskrba z električno energijo,
- klimatski pogoji,
- varnostne kopije,
- vzdrževanje opreme in
- vzdrževalna dela.

Kot tudi navaja Fabiani (2013) prinaša računalništvo v oblaku v javno upravo prednosti kot so večja učinkovitost in fleksibilnost, nižji stroški IT virov, boljše sodelovanje med ministrstvi in oddelki, večja možnost dela od doma ali s terena, boljša interakcija z državljani, hitrejša odzivnost na zahteve in bolj inovativne ter dostopnejše storitve. Po oblikovanju strategije in v skladu z veljavno zakonodajo je potrebno izvesti javni razpis za izbiro ponudnika oblačnih storitev, kar lahko traja več mesecev. Po izboru je potrebno ponudnika ustrezno preveriti, narediti analizo tveganja, zagotoviti ustrezne pogodbene dogovore in raven storitve. Šele na podlagi vseh zagotovljenih kriterijev se lahko začne postopek integracije oblaka v obstoječe sisteme.

5.2. OBLIKOVANJE MODELA USPOSABLJANJA ZAPOSLENIH ZA VARNO UPORABO OBLAČNIH STORITEV

5.2.1. GRADNIKI MODELA USPOSABLJANJA

Model usposabljanja zaposlenih za varno uporabo oblačnih storitev (Slika 6) prikazuje pomembne gradnike modela, ki so kombinacija usposobljenega osebja, postopkov in tehnologije ter navodil oziroma informacij, s katerimi se lahko zagotovi varnost poslovnega okolja. Kot smo že omenili, je za varovanje informacij zelo pomembna tudi izvedba sistema SUVI, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju varovanja informacij. Kot pomemben povezovalni element je zelo pomembna ozaveščenost o varnosti oziroma o varni uporabi oblačnih storitev. Kot smo že omenili, je zelo pomembno tudi opolnomočenje zaposlenih, saj na ta način dobijo znanja, informacije in veščine, ki jim omogočajo, da so zmožni sprejeti odločitve in zanje tudi odgovarjati. Zaposleni se morajo zavedati pomembnosti svoje vloge pri izvajanju del in nalog, zato morajo vedeti, na koga se lahko obrnejo, v kolikor naletijo na težave ali opazijo kakršne koli grožnje kibernetske kriminalitete.

Grafični prikaz modela nam kaže, kako lahko z ustreznimi gradniki, ki so med seboj povezani, zaposlene ves čas usposabljamo in informiramo oziroma ozaveščamo o pomembnosti varne uporabe oblačnih storitev in kako ustrezno pristopiti k reševanju problemov v primeru različnih nepravilnosti. V nadaljevanju si bomo natančneje ogledali posamezne gradnike modela, ki pa so, kot smo že omenili, med seboj povezani.

Najprej bi omenili usposobljenost osebja, tako zaposlenih kot tudi zunanjih sodelavcev. Glede na velikost in organiziranost podjetja je odvisno, kdo bo imel sploh dostop do določenih informacij. Egan in Mather (2005) navajata, da imajo večje družbe ponavadi posebne oddelke za varovanje informacij, na primer oddelek za informacijsko tehnologijo, v katerem so odgovorni za določitev varnostne strategije in izvedbo varnostnega programa. Omeniti pa je potrebno, da morajo imeti vsi zaposleni, od začetnikov do vodstvenega kadra, pomembno vlogo pri zagotavljanju uspeha varnostnega programa, zato je usposabljanje osebja za varno uporabo oblačnih storitev še kako pomembno.

Poleg usposobljenosti osebja so zelo pomembni dobri postopki, standardi in različni pravilniki, torej postopki varovanja informacij, ki so eden izmed pomembnih gradnikov učinkovitega usposabljanja varovanja informacij. Postopki, ki vsebujejo podrobna navodila, so zaposlenim v pomoč pri izvajanju njihovih del in nalog in to na varen način. Varnostni procesi, kot navajata Egan in Mather (2005), lahko vsebujejo podrobne postopke za zahtevanje dostopa do ključnih sistemov, saj mora prosilec izpolniti določene obrazce, da si zagotovi odobritev, preden mu osebje področja informacijske tehnologije dovoli dostop. Redno posodabljanje varnostnih pravilnikov je zelo pomembno, saj se grožnje ves čas spreminjajo.

Nenazadnje je za varno uporabo oblačnih storitev oziroma varovanje informacij zelo pomembna tehnologija. Vendar je potrebna velika previdnost, saj se lahko zaradi velike

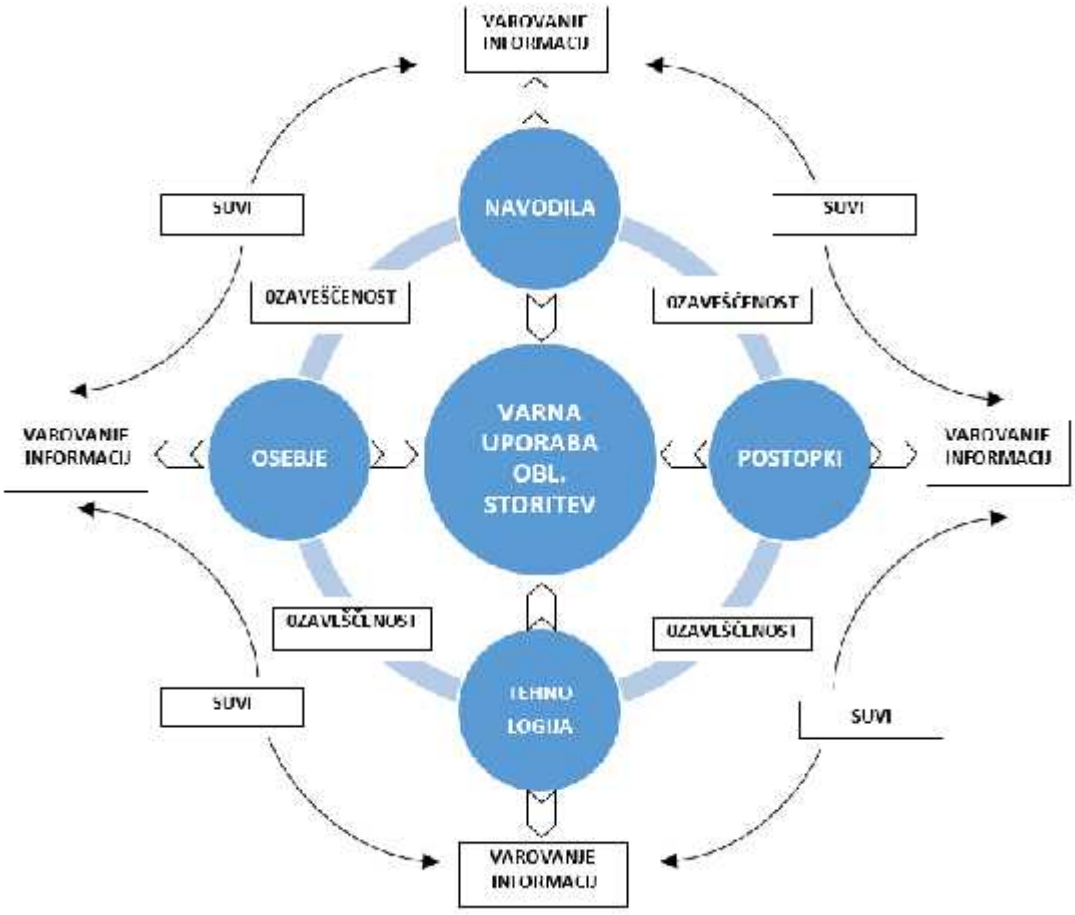
poplave različnih ponudnikov, ki seveda zagotavljajo, da bo njihova tehnologija izpolnila želeno varovanje informacij, spregleda bistveno dejstvo, da sama tehnologija še nikoli ni in tudi ne bo rešila težav z varnostjo.

Vodstveni kader mora (Egan in Mather, 2005) v organizaciji zagotoviti ustrezne komponente tehnologije, kot so:

- preverjanje pristnosti, pooblaščanje in vodenje računov (AAA –Authentication, Authorization, Accounting);
- požarni zidovi / virtualna zasebna omrežja (VPN – Virtual Private Networks);
- protivirusna programska oprema;
- upravljanje pomanjkljivosti;
- zaznavanje vdorov;
- filtriranje vsebine;
- šifriranje.

Model je zasnovan kot proces, kot krožni sistem, ki se nikoli ne konča. Zaradi nenehnih novih in različnih hekerskih groženj, kot tudi novih zaposlenih ali pa nadgrajene in izboljšane tehnologije je pomembno, da se izobraževanje in usposabljanje zaposlenih za varno uporabo oblačnih storitev kontinuirano izvaja na vseh ravneh. Zaradi omenjenih sprememb, ki se v organizaciji pojavljajo, je pomembno, da odgovorni skrbijo tudi za posodabljanje postopkov, standardov in različnih pravilnikov, torej pomembnih gradnikov učinkovitega usposabljanja varovanja informacij, saj je s tem zaposlenim zagotovljena stalna pomoč pri izvajanju njihovih del in nalog. Da pa se zaposleni zavedo pomembnosti varne uporabe oblačnih storitev in udeležbe pri izobraževanjih in usposabljanjih v zvezi s to problematiko, jih je potrebno stalno ozaveščati o pomenu varne uporabe oblačnih storitev in varovanja informacij nasploh. Za varovanje informacij je zelo pomembno tudi stalno izvajanje sistema SUVI, saj vemo, da v organizaciji poleg vpeljave in vzdrževanja skrbi tudi za nenehno izboljševanje delovanja na področju varovanja informacij.

Zaključimo lahko, da je poleg vseh gradnikov modela pomembno tudi zaupanje v operacijski sistem, strojno opremo in programsko opremo, zaupati pa moramo tudi ponudniku računalništva v oblaku kot tudi samemu osebju oziroma zaposlenim v organizaciji, saj vemo, da je človeški faktor zelo pomemben element pri varovanju informacij.



Slika 6: Model usposabljanja zaposlenih za varno uporabo oblačnih storitev

5.2.2. VSEBINE IN IZVEDBA USPOSABLJANJA ZAPOSLENIH

V nadaljevanju bomo prikazali poenostavljen primer e-izobraževanja v obliki ekranskih slik z naslovom »*Varna uporaba oblačnih storitev*« - *spletno izobraževanje*«. Izobraževanje je primerno za vse organizacije, ki pri svojem delu uporabljajo oblačne storitve oziroma poslujejo preko spleta.

Izobraževanje se prične s povabilom vseh zaposlenih po e-pošti, kjer je predstavljena tema izobraževanja, torej varnost informacij v oblačnih storitvah. V povabilu je na kratko opisano, kaj oblačne storitve so, komu je izobraževanje namenjeno in kakšen je njegov izobraževalni cilj. Pomembna podatka sta tudi predviden čas za izvedbo celotnega izobraževanja, vključno z zaključnim testom, in spletni naslov za dostop. Omenjena je tudi mejna vrednost uspešnosti opravljenega testa, ki je 80%. Vsak zaposleni si čas izobraževanja določi sam (glede na njegovo naravo dela oz. delovno mesto, ki ga zaseda), pomembno pa je, da ne prekorači končnega roka za uspešno opravljanje zaključnega preverjanja znanja oziroma testa.

Slika 7: Predstavitev učne vsebine

Podobno kot po e-pošti poslano vabilo za spletno izobraževanje je zasnovana tudi uvodna stran izobraževalnega modula (Slika 7), ki vključuje kratko predstavitev učne vsebine, cilj izobraževanja, kdo je ciljna skupina in kakšen je predviden čas potreben za izvedbo celotnega izobraževanja vključno z zaključnim testom.

Kot smo omenili že v preteklih poglavjih, je ozaveščanje zaposlenih o pomenu varovanja informacij in informacijskih sredstev podjetja, v katerem so zaposleni, izrednega pomena, saj so, kot navaja Rakovec (2005), poleg kapitala, naravnih virov in znanja zelo pomemben vir podjetja. Zaposleni so informacije in informacijska sredstva dolžni varovati pred pretečimi nevarnostmi in na ta način zagotavljati tako neprekinjeno poslovanje kot preprečevanje ali zmanjšanje kakršnekoli poslovne škode, ki bi jo podjetje lahko utrpelo.

Spletno izobraževanje je sestavljeno iz štirih tematskih sklopov.

1. Kaj je informacija?
2. Informacijska varnost
3. Sistem upravljanja varovanja informacij
4. Osnovni ukrepi varovanja informacij.

Osnovno spletno izobraževanje »Varna uporaba oblačnih storitev« se izvaja vsako leto in je obvezno za vse zaposlene.
Predviden čas, v katerem naj bi se zaposleni seznanili s celotno učno vsebino in opravili zaključno preverjanje znanja, je 30 minut.

Slika 8: Kaj je informacija?

Prvi sklop izobraževalnega modula (Slika 8) zaposlene pouči o pojmu informacija, kje se vidi njena kakovost, v kakšni obliki se lahko pojavlja in pred čem jo je potrebno varovati.

Zaposleni spoznajo, da je informacija podatek oziroma sporočilo, ki prejemniku poveča znanje ter tako vpliva na njegove odločitve in ravnanje Mohorič (1999), in da ga lahko uporabi takoj ter da se njena kakovost vidi v: točnosti, popolnosti, relevantnosti, dosegljivosti, preverljivosti, dostopnosti in varnosti.

Ne glede na to v kakšni obliki in po katerem sredstvu so prenesene, jih je potrebno, kot omenja Rakovec (2005), primerno varovati. Varovati jih je potrebno pred krajo, nepooblaščenim dostopom, izgubo, uničenjem ali potvarjanjem v vseh fazah njihovega življenjskega cikla (nastanek, shranjevanje, obdelava, prenos in uničenje).

Slika 9: Pomen varovanja informacij

Kot že omenjeno, je neodvisno od tega, kako so informacije prenesene, pomembno, da so primerno varovane upoštevajoč tri osnovna načela varovanja informacij, kot so zaupnost, celovitost in razpoložljivost (Slika 9), ki smo jih že predhodno natančno opredelili (glej str. 2).

Zelo pomembno je, da se zaposleni seznanijo s tem, da varovanje informacij obsega varovanje vseh pomembnih informacij in sredstev, ki so pomembna za nemoteno delovanje organizacije, in sicer: programska in strojna oprema, postopki in komunikacijske poti, itd. (Rakovec, 2005).

Slika 10: Sistem upravljanja varovanja informacij – SUVI

Kot doslej že večkrat omenjeno, sistem upravljanja varovanja informacij (SUVI) po standardu ISO/IEC 27001 (Slika 10) ponuja najboljše prakse za zagotovitev tehničnih ukrepov varovanja podatkov in informacijskih sistemov ter hkrati preko organizacijskih ukrepov skrbi za boljšo ozaveščenost zaposlenih (Astec, 2016).

V tem izobraževalnem modulu zaposleni spoznajo, da lahko vpeljava sistema SUVI prinese naslednje koristi (TEST IT, 2016):

1. porazdelitev odgovornosti za varno ravnanje s podatki in informacijami,
2. optimizacijo sredstev potrebnih za distribucijo in zaščito podatkov in informacij,
3. učinkovitejšo zaščito intelektualne lastnine organizacije (knowhow, patenti, poslovne skrivnosti),
4. zgodnje odkrivanje groženj, ranljivosti in potencialnih negativnih učinkov na poslovanje podjetja,
5. povečanje poslovne kredibilnosti in zaupanja s strani naročnikov ter dobaviteljev,
6. skladnost z zakonskimi zahtevami in standardi,
7. lažji prodor ali obstoj na mednarodnem tržišču,
8. mednarodno potrditev dobre poslovne prakse podjetja.

Slika 11: Osnovni ukrepi varovanja informacij

Slika 12: Osnovni ukrepi varovanja informacij

Omenimo naj, da ima varovanje informacij v dobi elektronske pošte, virusov in zlonamernih hekerskih napadov vedno večji pomen, saj nevarnosti prežijo ves čas na vsakem koraku. Zavedati se je potrebno, da so, kot omenja Krkoč (2009), uhajanje zaupnih informacij preko elektronske pošte, morebitne notranje ali zunanje zlorabe informacijskih virov ali zgolj malomarnost oziroma nevednost zaposlenih, le primeri različnih nevarnosti.

S predstavitvijo osnovnih ukrepov varovanja informacij (Slika 11-12) so tako vsi zaposleni seznanjeni s tem, kako ravnati v konkretnih primerih, kot so: vstop v varovani prostor, varovanje elektronskih in fizičnih sredstev, okvara, kraja ali izguba izmenljivih nosilcev podatkov, nosilcev podatkov neznanega ali sumljivega izvora ali suma namestitve zlonamerne programske opreme, kaj storiti v primerih, ko nosilcev izmenljivih podatkov ne potrebujejo več ali pa so ti postali neuporabni. Seznanijo se tudi z načelom čiste mize in praznega zaslona, kakšna je ustrezna uporaba elektronske pošte, kakšna so pravila pri nameščanju in vzdrževanju programske opreme, dostopnih pravicah in kako sestaviti dobro geslo in si ga pri tem tudi z lahkoto zapomniti. Kot pomoč pri sestavljanju ustreznih gesel, si lahko uporabnik pomaga tudi z različnimi generatorji gesel, za primer pa navajamo sledečega, ki je dostopen na spletni povezavi *http://passwordsgenerator.net/*. Na tej spletni povezavi pa lahko uporabnik preveri, kako močno geslo je ustvaril: *https://howsecureismypassword.net/*.

Slika 13: Zaključno preverjanje znanja - TEST

Z reševanjem kratkega zaključnega testa (Slika 13-14) se pri zaposlenih preveri, če podano vsebino razumejo. Možnih je več ponovitev izobraževanja, zaključi pa se z

dnem, ki je določen za zaključek obveznega letnega izobraževanja in preverjanja na temo varne uporabe oblačnih storitev.

Slika 14: Zaključno preverjanje znanja – TEST –Primer Vprašanje št. 7

Posamezno vprašanje je namenjeno dodatnemu utrjevanju pridobljenega ali samo osveženega znanja zaposlenih, pri tem pa dobijo tako sami kot organizator izobraževanja tudi občutek o stopnji usposobljenosti za varno uporabo oblačnih storitev. Vprašanja se nanašajo na učno vsebino, ki je predhodno predstavljena. Vsako vprašanje je na svojem ekanu, tako kot npr. na ekranski sliki 8, pod vprašanjem so nanizani različni pravilni in nepravilni odgovori. Kjer je možnih več pravilnih odgovorov, je to tudi posebej navedeno. Rezultat opravljenega testa je viden ob zaključku. Zaposleni po končanem reševanju testa pravilnih in napačnih odgovorov ne vidijo (vidi jih samo organizator izobraževanja).

6. DISKUSIJA

Izdelali smo pregled literature in analizirali človeške vidike varnosti v oblačnih storitvah. Na podlagi pregledane literature različnih avtorjev (Jurič, Frece, Hertiš & Srdič, 2009; Plummer, 2009; Marks & Lozano, 2010) lahko zaključimo, da je zelo pomembno, kako dobro so uporabniki seznanjeni z računalništvom v oblaku oziroma ozaveščeni o varni uporabi oblačnih storitev. Računalništvo v oblaku sicer ni nekaj novega, saj ga je že ob nastanku predhodnika današnjega spleta napovedal ameriški znanstvenik in začetnik internetnih povezav Leonard Kleinrock, ki je predvideval, da bo z razvojem omrežij računalništvo postalo storitev, ki bo vsem po potrebi vedno na voljo. Računalništvo v oblaku tako omogoča, da so digitalni podatki dostopni kjerkoli in kadarkoli, to pa ima seveda tudi močan vpliv na življenje vsakega posameznika kot tudi organizacije, saj so uporabniki oblačnih storitev zelo izpostavljeni in ranljivi. Ker so podatki, tako poslovni kot zasebni, lahko lahek plen nepooblaščenih uporabnikov, je še kako pomembno, da se uporabniki držijo določenih pravil in s tem zmanjšujejo tveganja, ki ga računalništvo v oblaku prinaša.

Na podlagi *NISTa* smo natančneje opisali 5 bistvenih značilnosti, ki oblikujejo oblačne storitve (*samopostrežnost, širok dostop preko omrežja, združevanje virov, hitra prilagodljivost in merljiva storitev).* Pri pregledu literature je tako najpogosteje zaslediti, da oblačne storitve sestavljajo tri »plasti« oz. storitveni modeli. Kot omenjajo različni avtorji (Mell & Grance, 2009; Jurič et al., 2009; Sheehan, 2009; Čehovin, 2011), so to: *Infrastruktura kot storitev* (IaaS, ang. *Infrastructure as a Service), Platforma kot storitev* (PaaS, ang. *Platform as a Service)* in *Programska oprema kot storitev* (SaaS. ang. *Software as a Service).* Prav tako pa avtorji (Voorsluys, Broberg & Buyya, 2011; Tomšič, 2011; Marks & Lozano, 2010; Höllwarth, 2012,) opredeljujejo izvedbene modele kot *javni, skupnostni, zasebni* ali *hibridni oblak.*

Predstavili smo najpomembnejše koncepte varnosti, ki so uveljavljeni in so usmerjeni na človeške vidike varnosti. V literaturi (Meier 2003; Palsit, 2016; Mell & Grance, 2011) smo zasledili, da celovit pristop ohranjanja informacijske varnosti zagotavljajo številne razsežnosti, tri glavne dimenzije pa so: *zaupnost*, *celovitost* in *razpoložljivost*. S strani ponudnika storitve je varnost zagotovljena tako, da nima niti dostopa niti vpogleda v podatke svojih uporabnikov. Na podlagi pregledane literature (Gradišar, 2003; Cachin & Schunter, 2011; Božič, 2011) lahko tudi zaključimo, da se varnost ne nanaša samo na strojno, programsko in drugo opremo, temveč se nanaša tudi na različne procese, delovne razmere in okolje ter dobro organizacijo in usposobljenost vseh zaposlenih kot tudi zunanjih partnerjev. Naloga varnosti je torej predvsem varovanje podatkov, kadar se ti prenašajo po omrežju, in pa tudi sama zaščita računalniškega sistema pred nepooblaščenim dostopom določenega uporabnika. Navedli smo dvajset varnostnih priporočil, ki jih je potrebno upoštevati za varnost računalništva v oblaku (Antonopoulos & Gilliam, 2010,), kljub temu pa moramo ponovno poudariti, da pravzaprav absolutno varnega sistema ni.

Opredelili smo eno izmed najbolj pogosto podcenjenih in hkrati najnevarnejših metod zlorabe človekovega zaupanja, in sicer socialni inženiring, ki je zlasti uspešen v povezavi z uporabo modernih tehnologij. Socialni inženiring po svoji naravi pomeni predvsem pridobivanje določenih koristi z zlorabo zaupanja posameznika oz. z manipulacijo. Najbolj razširjene metode socialnega inženiringa so prijateljstvo, elektronska pošta, pregledovanje smeti, pregled pisarn, zloraba zaupanja in čas. V zasebnem svetu posamezniki pogosto uporabljajo storitve, za katere se niti ne zavedajo, da delujejo kot oblačna storitev. Kot primer lahko navedemo elektronsko pošto Gmail, ki deluje transparentno za končnega uporabnika. Varnostna področja Vidmar (2011) deli na: zanesljivost sistema, zaščito sistema ter nadzor in upravljanje. Vsako področje je v nalogi natančno opredeljeno.

Natančno smo opredelili tudi oblačne storitve v bančništvu. Trenutna gospodarska kriza od bank zahteva, da so fleksibilne, še posebej pri znižanju stroškov informacijske tehnologije, vendar se banke zavedajo, da ne za ceno kakovosti. Nižji stroški informatike se kažejo kot najbolj očitna prednost računalništva v oblaku. Z oblačnimi storitvami si banke tako znižajo stroške, kar je eden bistvenih razlogov za uvedbo oblačnih storitev, hkrati pa zagotavljajo varno, donosno, hitro ter prilagodljivo bančno poslovanje skladno z zakonskimi zahtevami. Po navedbah Hőllwartha (2012) mora imeti banka, ki iznaša podatke, stalen nadzor nad svojo osrednjo dejavnostjo. V zvezi s tem smo navedli primere, kako imajo to urejeno v Nemčiji, Avstriji, Švici in v Sloveniji. Kljub vsem prednostim, ki jih nudi oblak, organizacije ne smejo pozabiti na varnost.

Kot primer lahko omenimo kibernetsko kriminaliteto, in sicer goljufije povezane s plačilnim prometom, kjer storilci praviloma izrabljajo šibke točke digitalnih plačnih transakcij. Ugotovili pa smo, da se problema varovanja informacij ne da reševati samo s tehničnimi ukrepi, zato je potreben celovit pristop, tako v okviru informacijske tehnologije, kot tudi z drugimi ukrepi, postopki, standardi, kontrolami in nadzorstvi.

Razložili smo enega od možnih načinov sistematične vpeljave oblaka v organizacijo (Markelj & Bernik, 2011), prav tako pa tudi podrobneje razčlenili sistem SUVI, ki na področju varovanja informacij v organizaciji skrbi za *vpeljavo, vzdrževanje* in *nenehno izboljševanje*, temelji pa na NSPU modelu Demingovega kroga v fazah Načrtuj – Stori – Preveri in Ukrepaj (Brezavšček & Moškon, 2010). Zaradi tesne povezanosti informacij, informacijske tehnologije in poslovnih procesov lahko zaključimo, da tak način delovanja prinaša tudi nove zahteve za varno, zanesljivo in dolgoročno uspešno poslovanje, kljub temu pa lahko zaključimo, da smo ljudje z vidika varnosti eden najšibkejših členov informacijskih sistemov.

Opredelili smo pomembnost opolnomočenih zaposlenih (Geroy, Wright & Anderson, 1998; Daft & Noe, 2001) in njihove ozaveščenosti o pomenu varne uporabe oblačnih storitev ter o možnih interventnih pristopih, da spremenijo določene vedenjske vzorce oziroma, da opustijo stare navade ter sprejmejo nov način vedenja (Kaplan, 1991; Demšar Pečak, 2014). Prav zato je izrednega pomena, da v organizacijah zaposlenim ves čas nudijo različna izobraževanja, tehnično podporo in pomoč, še prav posebej pa morajo biti pozorni na njihovo psihično oziroma duševno zdravje. Opredelili smo

psihološke vidike varnosti v virtualnem prostoru. Omenili smo pomen duševnega zdravja in vpliv stresa na celotno biopsihosocialno naravo človeka (Demšar Pečak, 2014).

Notranje osebje, torej zaposleni, predstavljajo največje tveganje in lahko povzročijo največ škode, kljub temu pa se najpogosteje zanemarjajo kot varnostna grožnja. Omenimo lahko, da se določeni podatki oziroma informacije poškodujejo ali uničijo zato, ker zaposleni in drugi vpleteni niso izučeni ali pa so nevešči uporabe, torej informacije ogrozijo nenamerno. Zaradi prevelike preobremenjenosti in stresa na delovnem mestu lahko pri zaposlenih pride do različnih psihosomatskih obolenj in drugih psihičnih motenj, to pa lahko pripelje do neustreznega, nenatančnega oziroma slabo opravljenega dela, deviantnega vedenja ali celo kriminalnih ravnanj – tudi v kibernetskem prostoru. Pri obravnavi storilcev kibernetske kriminalitete smo posebej izpostavili *antisocialno*, *mejno* in *narcistično* osebnostno motnjo. Največkrat so povzročitelji kriminalnih dejanj nezadovoljni zaposleni ali pa nekdanji zaposleni, njihov motiv je najpogosteje maščevanje zaradi domnevnih krivic. Takšne osebe imajo precejšnje znanje o delovanju organizacije, pogosto imajo tudi visoko stopnjo dostopa do občutljivih sistemov in podatkov. Najpogosteje so zaposleni na področju informacijsko komunikacijskih tehnologij in zato dosegajo nezanemarljivo stopnjo tehnične usposobljenosti (Bratuša, 2006).

Navedli smo, da posamezniki poškodujejo ali uničijo podatke namerno, na primer s kršenjem pravil in zakonov, in izrabljajo sistem v svojo korist, kot na primer kriminalci oz. kriminalne skupine, ki z informacijami trgujejo in jih zlorabljajo. Omenili smo profesionalne vsiljivce ali hekerje, ki svoje nepooblaščene vdore sproti prilagajajo in vedno znova odkrivajo pomanjkljivosti v programski oziroma strojni opremi, zato se je proti njim nemogoče popolnoma zavarovati. Na podlagi literature (Rogers v Bratuša, 2006) smo hekerje razvrstili v več skupin, in sicer na: novince, kiber-huligane, koderje virusov, malenkostne tatove, hekerje stare šole, profesionalne kriminalce in notranje osebje.

Različne zlorabe oblačnih storitev lahko prizadenejo tako posameznike kot tudi organizacije, zato smo analizirali primere delovanja posameznikov in skupin, ki so povzročili varnostne incidente v oblačnih storitvah in tako prizadeli posameznike ali organizacije. V nalogi smo kot primer zlorab, ki so prizadele posameznike, omenili kanadsko spletno stran Ashley Madison, ki se uporablja za spletno varanje svojih partnerjev. Zaradi zlorabe razkritja podatkov uporabnikov omenjene spletne strani je iz obupa prišlo celo do dveh samomorov in primerov izsiljevanja. Kot primere zlorab, ki so prizadele organizacije, smo omenili nekaj odmevnejših primerov vdorov v različne pomembnejše sisteme, ki so jih izvedli Kevin Mitnick, Adriano Lamo, Kevin Poulsen in Jonathan James. Posamezniki ali skupine varnostne incidente povzročajo zaradi različnih ideologij, političnih prepričanj, družbeno-kulturnih vplivov, verskega prepričanja in drugih vzrokov (Radcliff v Bratuša, 2006).

Med posamezniki, ki so povzročili varnostne incidente, smo omenili Juliana Paula Assangea, predstavnika WikiLeaksa, mednarodne neprofitne medijske organizacije, in

Edwarda Josepha Snowdna, ameriškega obveščevalca in žvižgača. Julian Paul Assange je leta 2010 javno objavil videoposnetek helikopterja Združenih držav Amerike kako strelja na civiliste in novinarje Reutersa v Iraku (Krečič, 2013). Edward Joseph Snowden, bivši pogodbeni sodelavec ameriške nacionalne varnostne agencije NSA, je junija leta 2013 razkril informacije o ameriškem nadzorovanju telefonskih in spletnih informacij v ZDA.

Med skupinami smo omenili Projekt Panama Papers, čigar razkriti notranji dokumenti odvetniške družbe Mossack Fonseca s sedežem v Panami vsebujejo informacije o 214.488 poslovnih subjektih s sedežem v tujini in so povezani z ljudmi v več kakor 200 državah in ozemljih. Družba je ena od najuspešnejših svetovnih ustanoviteljic navideznih družb v davčnih oazah, torej oblike podjetniškega poslovanja, s katerim je mogoče prikriti lastništvo premoženja in si s tem zmanjšati davčne odhodke. Omenili smo tudi primere hekerskih skupin Masters of Deception, Milworm in Anonymous po Dimc & Dobovšek (2012).

Opredelili smo varno uporabo oblačnih storitev in zgodnje zaznavanje nevarnega obnašanja zaposlenih pri uporabi oblačnih storitev in oblikovali model izobraževanja in usposabljanja zaposlenih za varno uporabo oblačnih storitev, saj se lahko posledice, kjer sistemi obstoječih kontrol človeškega aspekta ne zaznajo ali ne morejo zaznati visokega tveganja, kažejo tudi v izgubi premoženja, ugleda dostojanstva ali celo življenja.

Glede na to, da zaposleni in zunanji sodelavci predstavljajo največje tveganje oziroma največjo grožnjo informacijam, je zelo pomembno, da se lahko občutljive informacije in podatke pred zaposlenimi in drugimi osebami (npr. vzdrževalci) zavaruje z različnimi ukrepi, kot npr. natančnim pregledom preteklih aktivnosti in zaposlitev bodočega novo zaposlenega, preveritev pogodb z oskrbovalci sistema in ugotovitev, ali oni preverjajo preteklost svojih zaposlenih, itd. Poleg tega pa je potrebno za varnost usposobiti zaposlene, da zmorejo prepoznati sumljive dejavnosti, ki so jih takoj dolžni poročati nadzornemu osebju, prav tako pa morajo biti navodila in postopki za uporabo sistema in programov natančno določena. Izobraževanje in usposabljanje zaposlenih za varno uporabo oblačnih storitev je v organizacijah ključnega pomena, prav tako pa je pomembno, da se izobraževanj udeležujejo vsi zaposleni v organizaciji in poslovni partnerji. Izobraževanja se razlikujejo glede na to, komu so namenjena, saj gre lahko za usposabljanje vodstva, delavcev ali pa tudi ključnih uporabnikov informacijskih sredstev. Zelo pomembno je tudi, da se izobraževanja konstantno ponavljajo in dopolnjujejo. V nalogi smo opredelili različne vrste izobraževanj, saj lahko potekajo v obliki seminarjev ali delavnic, oziroma tudi seminarjev zaposlenih preko spletnega izobraževanja, torej interneta, kjer pridobivajo pomembna nova znanja o varnosti informacijskih sredstev.

Natančno smo definirali oblačne storitve v javni upravi in kot največjo oviro državnega oblaka izpostavili nenaklonjenost javne uprave spremembam, prav tako pa tudi neustrezne standarde v povezavi z varnostjo podatkov. Varnost podatkov je še toliko bolj pomemben dejavnik za javno upravo, saj pristojni državni organi shranjujejo in obdelujejo osebne podatke državljanov, zato lahko ob njihovi zlorabi pride do

katastrofalnih posledic (Catteddu & Hogben, 2012). Slovenska vlada je že leta 2008 začela pripravljati Strategijo učinkovite državne informatike, od februarja leta 2016 pa imamo v Sloveniji potrjen dokument z naslovom »Strategija kibernetske varnosti - vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti«. Kot primer dobre prakse, ki je javno dostopen na spletu, smo omenili »Priporočila informacijske varnostne politike javne uprave«, ki jih je na podlagi 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07 in 31/08), dne 28.10.2010 izdalo Ministrstvo za javno upravo, z namenom zaščite informacijskega premoženja, ki ga upravlja javna uprava. Dokument vsebuje 167. členov, ki jih morajo upoštevati tako vodstvo, zaposleni kot tudi osebe pogodbenih izvajalcev oziroma vsi, ki imajo dostop do omenjenega informacijskega premoženja.

Kot prispevek k znanosti smo oblikovali model izobraževanja in usposabljanja zaposlenih za varno uporabo oblačnih storitev. Model je zasnovan kot proces oziroma krožni sistem, ki se nikoli ne konča. Prikazuje pomembne gradnike modela, in sicer kombinacijo *usposobljenega osebja*, *postopkov* in *tehnologije*, ter *navodil* oziroma *informacij,* s katerimi se lahko zagotovi varnost poslovnega okolja. Zelo pomemben člen pri varovanju informacij je tudi sistem SUVI, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju varovanja informacij. V vlogi povezovalnega elementa je ozaveščenost o varnosti oziroma varni uporabi oblačnih storitev. Kot smo že omenili, je zelo pomembno tudi opolnomočenje zaposlenih, saj na ta način dobijo znanja, informacije in veščine, ki jim omogočajo, da so zmožni samostojno sprejeti odločitve in zanje tudi odgovarjati. Zaposleni se morajo zavedati pomembnosti vloge pri izvajanju svojih del in nalog, zato morajo vedeti, na koga se lahko obrnejo, v kolikor naletijo na težave ali opazijo kakršne koli grožnje kibernetske kriminalitete.

Na podlagi oblikovanega modela lahko zaključimo, da je poleg vseh njegovih gradnikov pomembno tudi zaupanje v operacijski sistem, strojno in programsko opremo, prav tako pa moramo zaupati tudi ponudniku računalništva v oblaku, kot tudi samemu osebju oziroma zaposlenim v organizaciji, saj vemo, da je človeški faktor eden najpomembnejših elementov pri varovanju informacij.

V zadnjem delu naloge smo pripravili poenostavljen primer spletnega izobraževanja z naslovom »*Varna uporaba oblačnih storitev*«. Uporabno je za vse organizacije, ki pri svojem delu uporabljajo oblačne storitve. Izobraževanje se prične s povabilom vseh zaposlenih po e-pošti skupaj z navodili. Poteka preko spleta, organizirano pa je tako, da nas na začetku v štirih ločenih sklopih pouči o izobraževalni temi in ob zaključku ponudi test. Z zaključnim testom preveri, koliko smo za to področje usposobljeni, da je test uspešno opravljen, pa je potrebno doseči vsaj 80%. Celotno izobraževanje je prikazano v ekranskih slikah.

Ozaveščanje zaposlenih o pomenu varovanja informacij in informacijskih sredstev podjetja, v katerem so zaposleni, je izrednega pomena, saj so zaposleni, poleg kapitala, naravnih virov in znanja, zelo pomemben vir podjetja. Zaposleni spoznajo, da je informacije potrebno primerno varovati v vseh fazah njihovega življenjskega cikla, pri

tem pa upoštevati vsa tri osnovna načela varovanja informacij: zaupnost, celovitost in razpoložljivost.

7. ZAKLJUČEK

V zadnjem času je zaradi razširjenosti oblačnih storitev še kako pomembno, da so podatki dobro zavarovani. Kot velja za varovanje različnih osebnih podatkov, ki jih želimo obvarovati, velja tudi za podatke v oblakih, saj vemo, da je glavna značilnost oblačnih storitev prenos podatkov in informacij preko različnih omrežij. Prav zato so podatki še toliko bolj izpostavljeni vdorom nepooblaščenih uporabnikov, ki se na nedovoljen način želijo dokopati do informacij. Seveda moramo omeniti, da pravzaprav absolutno varen sistema ne obstaja, saj je stopnja varnosti odvisna od nevarnosti, ki sistemu in uporabnikom objektivno grozijo, teh nevarnosti pa je vsak dan vse več v različnih oblikah.

Na žalost je ozaveščenost uporabnikov o varni uporabi oblačnih storitev običajno na zelo nizki stopnji, zato se velikokrat zgodi, da uporabniki napačno ravnajo tudi zaradi svoje neodgovornosti. Poleg tega lahko pride do uničenja ali poškodb določenih informacij tudi zato, ker zaposleni in drugi vpleteni niso usposobljeni za varno uporabo oblačnih storitev, torej ogrozijo informacije nenamerno. Zaposleni o različnih postopkih in izvedbah določenih procesov velikokrat niso izučeni, jih ne poznajo ali pa o njih niso pravočasno obveščeni, zato nepooblaščeni uporabniki z zlorabo zaupanja, torej z uporabo socialnih veščin oziroma psiholoških tehnik, pridobijo določene podatke, ki jih nato uporabijo za pridobivanje večinoma finančnih koristi.

Vsekakor lahko zaključimo, da je najboljša obramba pred takimi napadi, kot omenja Bratuša (2006), »prav gotovo redno usposabljanje zaposlenih, ki jim je treba praktično ponazoriti, na kaj morajo biti pri delu pozorni in kateri podatki so še posebej pomembni. Poleg tega je zelo pomembno, da podjetje prilagodi varnostno politiko takim napadom, saj v nasprotnem primeru požarni zidovi in sistemi IDS ne zagotavljajo nikakršne varnosti«.

Na podlagi omenjenega lahko zaključimo, da smo ljudje z vidika varnosti eden najšibkejših členov informacijskih sistemov, zato mora organizacija poleg vlaganj v tehnologijo in druge varnostne sisteme velik del vlaganj nameniti tudi človeškim virom.

LITERATURA IN VIRI

Astec (2016). Uvedba ISO 27001 (SUVI). Pridobljeno 14.04.2016 na http://www.astec.si/informacijska-varnost/sistemi-vodenja/uvedba-iso-27001-suvi

Amnesty International(2015). Dve leti po obsodbi Chelsea Manning. Pridobljeno 14.06.2016 na http://www.amnesty.si/c-manning-2-leti-po-obsodbi

Antonopoulos, N., &Gilliam, L. (2010). Cloud Computing - Principles, System and Applications. London: Springer.

Auza, J. (2012). 7 Most Notorious Computer Hacker Groups of All Time Tech Source. Pridobljeno 15.6.2016 na http://www.junauza.com/2011/07/7-most-notorious-computer-hacker-groups.html

Božič, G. (2011). Ali ja kaj trden vaš oblak? Kaj nam prinaša računalništvo v oblaku?, Konferenca Arnes 2011. Zbornik člankov, 9-11

Bratuša, T. (2006). Hekerski vdori in zaščita. Ljubljana: Pasadena.

Brezavšček A., Moškon S. (2010). Vzpostavitev sistema za upravljanje informacijske varnosti v organizaciji. Uporabna informatika. 18(2).

Brodnik, A., Dobrin, A., Drobnič, M., Gams, M., Mohar, B., & Petkovšek, M. (1998). Računalništvo. Ljubljana: Cankarjeva založba.

Butina, M., (2010). Vreme? Oblačno! Dnevi slovenske informatike 2010. Portorož: Astec d.o.o.

Cachin, C., & M. Schunter. (2011). A cloud you can trust. How to ensure that cloud computing's problems—data breaches, leaks, service outages—don't obscure its virtues IEEE Spectrum 48 (12) 28-51. doi:10.1109/MSPEC.2011.6085778.

Carr, N., (2009). The big switch: rewiring the world from Edison to Google (lsted.). New York: W.W. Norton & Company, Inc.

Conger, J. A., & Kanungo, R. N. (1988). The Empowerment Process: Integrating Theory and Practice. The Academy of Management Review, 13(3), 471-482.

Crnović, D. (2015). Dva samomora zaradi razkritja uporabnikov spletne strani za varanje.Pridobljeno 14.05.2016 na http://siol.net/digisvet/novice/dva-samomora-zaradi-razkritja-uporabnikov-spletne-strani-za-varanje-393183).

Čehovin, G. (2011). Mladi podjetnik. Pridobljeno 14.04.2016 na http://mladipodjetnik.si/podjetniski-koticek/poslovanje/racunalnistvo-v-oblaku-fleksibilnejsi-dostop-do-racunalniskih-storitev

Daft, R. L., & Noe, R. A. (2001). Organizational behavior. Orlando: Harcourt Inc.

Demšar Pečak, N. (2014). Model socialnega marketinga pri reševanju problemov v partnerskem odnosu. Novo mesto: Fakulteta za organizacijske študije.

Dimc, M., & Dobovšek, B., (2012). Kriminaliteta v informacijski družbi

Egan M. & Mather T.(2005). Varovanje informacij- grožnje izzivi in rešitve.Založba Pasadena

Erzar, T. (2007). Duševne motnje: Psihopatologija v zakonski in družinski terapiji. Celje: Celjska Mohorjeva družba.

Fabiani, J. (2013). Računalništvo v oblaku v javni upravi. Univerza v Ljubljani. Fakulteta za družbene vede.

Gartner. (2011). Gartner Says Worldwide Software as a Service Revenue Is Forecast to Grow 21 Percent in 2011. Pridobljeno 14.4.2016 na http://www.gartner.com/it/page.jsp?id=1739214&M=6e0e6b7e-2439-4289-b697-863578323245.

Geroy, G. D., Wright, P. C., & Anderson, J. (1998). Strategic performance empowerment model. Empowerment in Organizations, 6(2), 57-65.

Gradišar, Miro. 2003.Uvod v informatiko. Ljubljana: Ekonomska fakulteta.

Gradišar, M., J. Jaklič, T. Damij & P. Baloh. 2005: Osnove poslovne informatike. Ljubljana: Ekonomska fakulteta.

Grobauer, B., T. Walloschek & E. Stocker. (2011). Understanding Cloud Computing Vulnerabilities. Security & Privacy, IEEE 9 (2): 50-57.

Huš, M. (2015). Na internetu arhiv z domnevnimi podatki s strani Asley Madison. Pridobljeno 14.04.2016 na https://slo-tech.com/novice/t650955.

Jurič, M. B., Frece, A., Hertiš, M. & Srdič, G. (2009). Priložnosti uporabe računalniškega oblaka v javni upravi. Informatika v javni upravi 2009. Brdo pri Kranju: Univerza v Mariboru, FERI in Center za računalništvo v oblaku ter Kompetenčni center za SOA.

Informacijski pooblaščenec. (2009). Socialni inženiring in kako se pred njim ubraniti? Pridobljeno 14.04.2016 na https://www.iprs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf

Informacijski pooblaščenec. (2012). Varstvo osebnih podatkov in računalništvo v oblakih. Pridobljeno 18.4.2016na https://www.iprs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf

Inštitut za razvoj človeških virov (2016).Pridobljeno 14.6.2016 na https://www.google.si/search?q=in%C5%A1titut+za+razvoj+%C4%8Dlove%C5%A1kih+virov&ie=utf-8&oe=utf-8&client=firefox-b&gws_rd=cr&ei=Zs-QV5HiGMv7UvaHseAK

Inštitut za produktivnost (2016). Pridobljeno 14.7.2016 na http://www.produktivnost.si/ja-ljudi-je-zal-treba-stalno-pritiskat-drugace-ni-nic/odnos-med-stresom-in-zmogljivostjo-zaposlenih-3/

Knorr, E. & Galen Gruman. (2016). What Cloud Computing Really Means. Info World. Pridobljeno 13.3.2016 na http://www.infoworld.com/article/2683784/cloud-computing/what-cloud-computing-really-means.html

Konec Juričič, N. (b.d.). Duševno zdravje. Pridobljeno 14.1.2016 na http://www.zzv-ce.si/dusevno-zdravje

Krkoč, P. (2009). Standardizirana vpeljava sistema neprekinjenega poslovanja (Specialistična naloga). Ljubljana: Fakulteta za varnostne vede.

Krečič, J. (2013). Julian Assange: »Wikileaks smo vohuni za ljudi.« (iz arhiva) Pridobljeno 13.06.2016 na http://www.delo.si/zgodbe/sobotnapriloga/julian-assange-wikileaks-smo-vohuni-za-ljudi.html.

Leskovar, R. (2011). Varovanje podatkov v oblaku in dileme v zvezi z varovanjem zasebnosti. Odgovornost v fizioterapiji:1. mednarodna znanstvena konferenca (zbornik izbranih referatov z recenzijami) (str. 26-36). Evropsko središče Maribor, Maribor

Lee, M., & Koh, J. (2001). Is empowerment really a new concept? The International Journal of Human Resource Management, 12(4), 684-695.

Markelj, B., & Bernik, I. (2011a). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav.

Markelj, B., & Bernik, I. (2011b). Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. konferenca Dnevi slovenske informatike, Portorož, Slovenija, 18.-20.april 2011. Ljubljana: Slovensko društvo Informatika.

Marks, E. A., & Lozano, B. (2010). ExecutivesGuide to CloudComputing. New Jersey: John Wiley & Sons, Inc.

Meier, J. D. (2003). Improving Web Application Security: Threats and Counter measures. Redmond, Wash: Microsoft Corporation. Pridobljeno 11. 2. 2016 na https://msdn.microsoft.com/enus/library/ff649874.aspx

Merljak, S. (2013). Žvižgači: Svet je nevaren zaradi tistih, ki nič ne naredijo. Pridobljeno 25.06.2016 nahttp://www.delo.si/novice/slovenija/zvizgaci-svet-je-nevaren-zaradi-tistih-ki-nic-ne-naredijo.html

Mešič, J. (2011). Varni na internetu. Kaj nam prinaša računalništvo v oblaku? Ljubljana: Arnes.

Milavec, M. (2010). Konvergenca in integracija medijev z uporabo računalništva v oblaku. Diplomsko delo Maribor.

Ministrstvo za javno upravo (2010). Priporočila informacijske varnostne politike javne uprave. Pridobljeno 11.5.2016 na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/DIES/IVPJU_01.pdf

Mohorič, T. (1999). O podatku in informaciji. Pridobljeno 10.04.2016 na (http://lopes1.fov.uni-mb.si/IS/99/org/mohoric.pdf)

Obermayer B., Ryle G., Walker Guevara, M. & et al (2016). Pridobljeno 05.3.2016 na http://www.delo.si/svet/globalno/veliko-razkritje-financnih-dokumentov-povezanih-z-davcnimi-oazami-omogoca-vpogled-v-svet-globalnega-kriminala-in-korupcije.html.

Pahor, D., & Drobnič, M. (2002). Leksikon računalništva in informatike. Ljubljana: Založba Pasadena.

Palsit (2016). Vodenje varovanja informacij. Pridobljeno 15.03.2016 na https://www.palsit.com/slo/podjetje.php

PIS – Pravno-informacijski sistem. Sklep o ureditvi notranjega upravljanja, upravljalnem organu in procesu ocenjevanja ustreznega notranjega kapitala za banke in hranilnice. Pridobljeno 27.6.2016 na http://www.pisrs.si/Pis.web/pregledPredpisa?id=SKLE10628

PIS – Pravno-informacijski sistem. Zakon o bančništvu (ZBan-2). Pridobljeno 27.06.2016 na http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6716

Pohorec. S. (2011). Skrite pasti računalništva v oblaku. MonitorPRO. Pridobljeno 15.02.2016 na http://www.monitorpro.si/106191/praksa/skrite-pasti-racunalnistva-v-oblaku/

Plummer, D.C. (2009). Experts Define Cloud Computing: Canweget a Little Definition in our definitions? Gartner, Inc. Pridobljeno 15.02.2016 na

http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/

Republika Slovenija. URAD RS ZA VAROVANJE TAJNIH PODATKOV. Osnovno usposabljanje. Pridobljeno na http://www.uvtp.gov.si/si/delovna_podrocja/usposabljanje/osnovno_usposabljanje

Spreitzer, G. M. (1996). Social structuralcharacteristicsofpsychologicalempowerment.AcademyofManagementJournal, 39 (2), 483-504.

Strategija kibernetske varnosti, Vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti. Pridobljeno 20.05.2016 na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/Kakovost/Strategija_razvoja_JU_2015-2020/Strategija_razvoja_SLO_final_web.pdf

Wickisier, E. L. (1997). Theparadoxofempowerment - a casestudy. Empowerment inOrganizations, 5(4), 213-219.

Willis, J.M. (2008,). Who coined the phrase cloud computing? IT Management and Cloud Blog. Pridobljeno 05.02.2016 na http://www.johnmwillis.com/cloud-computing/who-coined-the-phrase-cloudcomputing/

Vidmar, T. (2011). Računalništvo v oblaku, 1.del: Teorija distribuiranih sistemov. Ljubljana: Založba Pasadena

Voorsluys, W., J. Broberg, & R. Buyya. (2011). Introduction to Cloud Computing. Cloud Computing: 1-41.

Selye, H. (1950). Stress and The General Adaptation Syndrome. British Medical Journal. London. 7 (17)

Simčič, M. (2011). Kaj sploh je računalništvo v oblaku. Moj Mikro, Pridobljeno 05.02.2016 na http://www.mojmikro.si/center/povem_naglas/kaj

Schmidt, A. (2003). Najmanj, kar bi morali vedeti o stresu. Ljubljana: samozaložba

Skukan, K. (1998). ZUNANJE IZVAJANJE: Rešitev ali potop? Uporabna informatika.

Šket, I. (2009).Psihološke implikacije kiberprostora ter interakcije med storilci in žrtvami: diplomsko delo. Fakulteta za varnostne vede. Univerza v Mariboru

Tomšič, A. (2011). Zasebnost v oblaku. Kaj nam prinaša računalništvo v oblaku? Zbornik člankov. Konferenca ARNES 2011. Pridobljeno 20.4.2016 na https://www.arnes.si/files/2015/10/konferenca-arnes-zbornik-2011.pdf

Test IT (2016). O ISO 27001 standardu. Pridobljeno 20.05.02016 nahttp://www.iso-27001.si/#aboutUs.

Uradni list (2007). ZAKON O VARSTVU OSEBNIH PODATKOV uradno prečiščeno besedilo (ZVOP-1-UPB1). Pridobljeno 28.06.2016 na https://www.uradni-list.si/1/content?id=82668

Vodič BITKOM-a, »Cloud Computing - Evolution in der Technik, Revolution in Business«, 2009

KAZALO SLIK

KAZALO TABEL