# Informacijsko varnostna politika na letališču

Sašo Žurga

**Namen**
Namen prispevka je izpostaviti najpomembnejša tveganja, ki se lahko pojavljajo na področju informacijske varnosti, obenem pa predlagati možne ukrepe s pomočjo katerih se je možno izogniti varnostnim incidentom.

**Metodologija**
V prispevku je uporabljena deskriptivna metodo, kjer sem s pomočjo virov opisal osnovne pojme. V nadaljevanju sem uporabil razlagalno metodo in kompilacijo.

**Ugotovitve**
V okviru službenih dolžnosti se morajo uveljaviti omejitve zaposlenim glede neopravičene uporabe ali zlorabe informacijsko komunikacijskih tehnologij, s katerimi bi morda namenoma ali ne namenoma lahko ogrozili ali škodovali informacijski varnosti znotraj letališča. Kot dodaten dejavnik na področju varovanjainformacij in sistemov se mora velik poudarek dati na ustrezni varnostni zaščiti sistemov, ki nadzorujejo in upravljajo letenje. Predstavljena informacijska varnostna politika nakazuje smernice za pripravo operativnih politik in predstavlja osnovo za razumevanje potrebnih postopkov.

**Izvirnost/pomembnost**
Ugotovitve prispevka so namenjene letalskim potnikom za razumevanje postopkov na letališčih, zaposlenim na letališčih, kot tudi upravam letališč, ki morajo kot vodstvo poskrbeti za izvajanje informacijsko varnostne politike letališča.

**Ključne besede**: informacije, informacijsko varnostna politika, letališča, varnost, potniki, osebje.

## 1 Uvod

Ker so letališča v tesni povezavi z varnim delovanjem informacijskih sistemov je potrebna temeljita ter takšna informacijsko varnostna politika, ki ščiti vitalne dele informacij ter podatkov za uspešno delovanje letališča. Le zaščita podatkov znotraj sistema, kot so na primer seznami potnikov, ne zadostuje dovolj, da bi lahko govorili o temeljiti zaščiti, ki nam jo zagotovi upoštevanje varnostne politike. Prav tako zaposleni s svojim ravnanjem pripomorejo k varovanju podatkov ter informacij znotraj in zunaj območja letališča. Razkritje zaposlenih tujim osebam osebno ali preko uporabe informacijsko komunikacijskih sredstev glede načinov in podrobnosti glede fizičnega in informacijskega varovanja znotraj območja letališča predstavlja veliko grožnjo varnosti na splošno. Tu navsezadnje gre za pretok velikega števila

ljudi, ki potujejo z varnimi pričakovanji glede varnosti. Vdori v informacijske sisteme na letališču ter nalaganje škodljive programske opreme v sisteme za nadzor letenja lahko odločajo o velikem številu ljudi. Zato se je potrebno osredotočiti na širši vidik varovanja tako informacij kot sistemov na letališču.

# 2 Informacijsko varnostna politika

## 2.1 Spoštovanje informacijsko varnostne politike

Z jasnimi usmeritvami vodstvenega kadra morajo vsi zaposleni spoštovati informacijsko varnostno politiko znotraj območja letališča. Na podlagi teh usmeritev morajo biti določene tudi disciplinske odgovornosti zaradi kršitev informacijsko varnostne politike letališča. Pri spoštovanju varnostne politike se ne smemo niti oddaljiti od tega, da podjetja, katera se soočijo že z morebitnim incidentom vdora v sistem, tega varnostnega dogodka ne prijavijo. Namreč pojavlja se prepričanje, da bi pri tovrstnem preboju varnostnega sistema, podjetje izgubilo zaupanje javnosti. Incident in njegova prijava bi se seveda posledično navezovala na prihodnost poslovanja podjetja (uprave letališča) (Dimc, 2009).
Na tem mestu je zato potrebno omeniti zavezanost teh podjetij prijaviti takšen varnostni dogodek ter s tem dokazati, da je samo podjetje pripravljeno in voljno upravičiti pričakovanja potnikov glede varnosti.

**Tveganje**

1. Nejasna disciplinska odgovornost zaposlenih zaradi kršitev informacijske varnostne politike s strani določb, ki jih poda vodstveni kader. Za posledico se šteje izguba podatkov, nepooblaščena izmenjava podatkov, ter izdajanje informacij in podatkov.

**Ukrepi**

1. Notranji akt naj predpiše obvezno spoštovanje informacijske varnostne politike ter določi disciplinsko odgovornost za njene kršitve.
2. Zaposleni morajo dobiti elektronski izvod informacijsko varnostne politike, da se seznanijo z določbami. Prav tako je potrebno zagotoviti dodatna izobraževanja s področja informacijskih sistemov.
3. Za implementacijo določb informacijske varnostne politike morajo biti uporabljena najnovejše dognanja s področja informacijske varnosti.

## 2.2 Varovanje zaupnih podatkov

Pri varovanju zaupnih podatkov je ključnega pomena seznanitev zaposlenih, da podatke, do katerih bodisi pridejo naključno ali v okviru službenih obveznosti, ne izdajajo zunaj letališke uprave. Ker je možen izliv pomembnih informacij tudi preko elektronske pošte, se jih poduči tudi o tem. S podpisom izjave o varovanju podatkov se zavežejo, da ne izdajajo informacij ali podatkov, ki so pomembni za delovanje letališke uprave.

**Tveganje**

1. Zaposleni lahko razkrijejo podatke bodisi o potnikih ali o drugih pomembnih in zaupnih informacijah, ki se tičejo same organizacije delovanja varnostnih mehanizmov znotraj letališča.

**Ukrepi**

1. S podpisom izjave o varovanju podatkov se zaposleni zavežejo za varovanje podatkov, ki so jih v času zaposlitve pridobili.

2. V primeru zunanjih izvajalcev, ki opravljajo delo znotraj letališke uprave, se njih prav tako opozori in s podpisom formalne izjave o varovanju podatkov obveže obveznosti, ki jih nalaga izjava. Kršitve določb iz te izjave se sankcionira.
3. V primeru prekinitve delovnega razmerja ali upokojitve so te osebe dolžne spoštovati določila o varovanju zaupnih podatkov.
4. Služba za odnose z javnostjo, ki deluje v okviru letališča in ima stik z mediji, lahko le ta v okviru, ki ji določajo pogoji obvešča medije in javnost o dogodkih in informacijah. Ostali zaposleni zaradi večje možnosti razkritja podatkov in informacij ne smejo odgovarjati na vprašanja medijev.
5. Izdajanje informacij družinskim članom ali znancem o zaupnih podatkih je prav tako prepovedano, kar je že navedeno s podpisom izjave o varovanju podatkov.
6. Najpogostejši izliv informacij in podatkov, ki so ključne narave za uspešno in varno delovanje letališke uprave, je elektronska pošta. Zaposlenim se tako mora onemogočiti možnost izdajanja informacij na ta način.

## 2.3 Primerna uporaba interneta

Uporaba interneta mora biti določena s strani vodstvenega kadra, ki določa v kolikšnem obsegu se lahko uporablja internet, predvsem pa za službene namene. S pomočjo interneta se ne sme prenašati datotek, kot so datoteke z neprimerno ali žaljivo vsebino. Obstajati mora podatkovna meja uporabe interneta, saj se lahko le na ta način zaustavi nehoteno ali hoteno prenašanje tudi datotek s škodljivo vsebino (Stallings, Brown, 2008).

**Tveganje**
1. Zaposleni preko interneta lahko nalagajo in distribuirajo vsebine, ki so neprimerne, žaljive in škodljive.

**Ukrepi**
1. Zaposlene se seznani katera vsebina je neprimerna in jih poduči o sankcijah v primeru kršitve.
2. S podatkovno mejo se lahko doseže zaustavitev prekomernega nalaganja vsebin, ki niso pomembne, niti niso povezane v okvir službenih obveznosti.
3. Nalaganje žaljive in neprimerne vsebine se ustrezno prepreči in sankcionira.

## 2.4 Seznanitev z informacijsko varnostno politiko

Z informacijsko varnostno politiko morajo biti seznanjeni vsi zaposleni. Novo zaposlene in zunanje izvajalce je potrebno še dodatno poučiti in izobraziti o delovanju in določbah informacijsko varnostne politike. Pogodba o zaposlitvi in izjava o varovanju podatkov morata vsebovati jasne določbe glede varovanja informacij in zaupnih podatkov.

**Tveganje**
1. Informacijsko varnostna politika se v okviru letališke uprave ne more izvajati, če zaposleni niso seznanjeni z določbami iz tovrstne politike.

**Ukrepi**
1. Pred pričetkom dela, torej ob sklenitvi pogodbe o zaposlitvi je potrebno bodočega sodelavca seznaniti z določbami informacijsko varnostne politike.
2. S podpisom izjave o varovanju podatkov se zaveže, da bo spoštoval določila, ki varujejo informacije in podatke znotraj letališke uprave (Ministrstvo za javno upravo, 2010).
3. Z določitvijo mentorja in dodatnim izobraževanjem se lahko zagotovi spoštovanje in upoštevanje določb informacijsko varnostne politike zaposlenih znotraj letališke uprave.

**2.5 Redno obveščanje o spremembah informacije varnosti**

Preko obvestil (elektronska pošta, interni bilten) je potrebno zaposlene obveščati o novostih na področju informacijske varnosti znotraj letališke uprave. Vse nove spremembe, ki se uveljavijo na področju lastne informacijsko varnostne politike se morajo ustrezno prenesti do zaposlenih na vseh nivojih. Ob vzpostavitvi ali bistveni spremembi vsakega informacijskega sistema je potrebnozagotoviti usposabljanje za vse zaposlene, da bodo lahko nov informacijski sistem uporabljaliučinkovito in ne bodo ogrožali informacijske varnosti.

**Tveganje**

1. Spoštovanje določil informacijsko varnostne politike se lahko skozi čas preneha dosledno upoštevati in obenem izvajati.
2. V primeru sprememb na področju informacijsko varnostne politike lahko zaradi nepoznavanja nove ureditve prihaja do resnih izgub informacij ali podatkov.

**Ukrepi**

1. preko obvestil in ustrezne komunikacije vodstvenega kadra z zaposlenimi je potrebno zagotoviti, da se spremembe, ki so bile uvedene na področju informacijsko varnostne politike, res uresničujejo.
2. Informacije, ki se navezujejo na spremembe in dopolnitve določb informacijsko varnostne politike, morajo biti dostopne vsem zaposlenim na vseh nivojih.
3. Zunanjim izvajalcem je potrebno ob prvem nastopu dela takoj zagotoviti informacije glede upoštevanja novih sprememb določb informacijsko varnostne politike.
4. Zaradi možnosti izgube ali uničenja podatkov je potrebno pravilno in jasno podati informacije o spremembah in dopolnitvah, saj je lahko napačna interpretacija razlog za nenamerno poškodovanje informacij ali podatkov.

## 2.6 Zaščita varovanega območja

Na področju informacijske varnosti se pojem 'varovano območje' nanaša na prostor, kjer se nahaja strojna oprema in nosilci podatkov. Pri pripravi varovanega območja je potrebno upoštevati zahteve proizvajalca strojne opreme. Varovano območje mora biti pripravljeno tako, da omogoča dostop samo pooblaščenim osebam z uporabo ustrezne tehnologije (npr. magnetne kartice).

**Tveganje**

1. Zlonamerna poškodba ali kraja nosilca podatkov lahko ogrozi uspešno delovanja letališke uprave.

**Ukrepi**

1. Območje, predvideno za namestitev opreme, je treba zavarovati pred nepooblaščenimi osebami.
2. Običajen dostop sme imeti le pooblaščeno osebje.
3. Javne storitve, kot so dobava električne energije, vode, telekomunikacije ipd., morajo biti nameščene tako, da se lahko preusmerijo na izbrano območje.
4. Preveriti je treba uporabo sosednjih prostorov glede ogrožanja občutljive računalniške opreme, kot npr. izogibanje bližine kuhinje, strojnice dvigal, servisnih delavnic ipd.
5. Struktura zgradbe mora biti požarno varna. To ocenjuje pristojni organ za požarno varnost, skladno s predpisi o graditvi objektov (MJU, 2010).

## 2.7 Zagotavljanje fizičnega varovanja

Zagotavljanje fizičnega varovanja območja morajo biti varovana pred nezakonitim ali nepooblaščenim fizičnim vstopom ali vdorom. Varovana območja so območja, kjer se nahajajo

podatki ali oprema, ki morajo biti zaradisvoje ključne vloge za letališče zavarovani pred nepooblaščenim dostopom. Dostop je zatodovoljen samo določenim osebam, ki dostop potrebujejo za svoje naloge. Nepooblaščen dostop zato pomeni tako dostop zunanjih oseb kot tudi dostop zaposlenih brezpooblastila.

**Tveganje**

1. Osebe lahko (včasih tudi neopazno) nezakonito vstopijo z namenom kraje, poškodovanja ali povzročanja drugih motenj v delovanju.

**Ukrepi**

1. Okolje varovanega območja mora biti zavarovano pred nepooblaščenim dostopom.
2. Potrebno je zagotoviti fizično varovanje tako informacijskih sistemov, kot fizično varovanje objekta, za slednjega poskrbi ministrstvo za notranje zadeve.
3. Tudi znotraj varovanega območja je potrebno dodatno zaščititi strežniško in komunikacijsko opremo. Običajno smejo imeti zaposleni dostop le do terminalov oziroma delovnih postaj.
4. Še posebej je potrebno omejiti dostop do delov varovanega območja, kjer so shranjene varnostne in arhivske kopije podatkov.
5. Opredeliti je treba intervencije, pri katerih je vstop v varovano območje dovoljen ob vsakem času.
6. Vsi zaposleni z dostopom v varovano območje morajo biti zavezani k molčečnosti (notranji akt pogodba o zaposlitvi, izjava o varovanju podatkov).

## 2.8 Varovanje omrežnih podatkov in storitev pred načrtnimi napadi in vdori

Zaposleni v letališki upravi morajo delovati tako, da bodo strojna oprema, programska oprema, podatki in procesi v največji možni meri zaščiteni pred načrtnimi napadi in vdori.
Predvsem zaradi odgovornosti, ki jo nosi letališka upravi pri prevozu potnikov je lahko zaradi vdora in namestitve škodljive programske opreme znotraj sistema za letenje usodno za človeška življenja.

**Tveganje**

1. Napačna ali pomanjkljiva namestitev programske opreme za varovanje omogoča zunanjim napadalcem vdor v informacijski sistem.

**Ukrepi**

1. Informacijski sistem naj bo zavarovan s programsko opremo, ki omogoča omejen in nadzorovan dostop iz interneta.
2. Z ustrezno programsko opremo je potrebno zaščititi sistem kontrole letenja, saj je v primeru namestitve škodljive programske opreme (trojanski konji) na ta sistem lahko letenje ovirano ali celo usodno.
3.Programska oprema naj bo nameščena strokovno in z vsemi popravki, ki jih priporoča proizvajalec programske opreme. Privzete nastavitve naj bodo spremenjene tako, da bo stopnja varnosti višja od privzete.
4. Pri internetu naj se prepreči dostop do strani, ki niso pomembne za delovanje letališča, saj je lahko v nasprotnem primeru možnost nezakonitega dostopa do sistema lažji.
5. V primeru napada na sistem ali vdora v sistem je potrebno razviti primerne postopke za zagotavljanje ustreznega zbiranja in zavarovanja dokazov, ki so nastali pri tem kaznivem dejanju.
6. Če so osumljeni zaposleni v organu, je potrebno sprožiti disciplinski postopek, kateremu lahko sledi prenehanje delovnega razmerja ali pregon (MJU, 2010).

### 2.9 Prijava varnostnih dogodkov

Zaposleni, pogodbeni sodelavci in zunanji izvajalci morajo vsak varnostni dogodek ali sum varnostnega dogodka nemudoma prijaviti službi za informatiko, da se zagotovi hitro in učinkovito ukrepanje za preprečitev škode in zavarovanje dokazov (Informationsecurity forum, 2003).

**Tveganje**

1. Če ni uveljavljen postopek za javljanje varnostnih dogodkov, zaposleni ne bodo poročali o teh dogodkih.

**Ukrepi**

1. Vse zaposlene znotraj letališke uprave mora notranji akt obvezovati k prijavi varnostnih dogodkov.
2. Nekatere od teh varnostnih dogodkov lahko samodejno javlja informacijski sistem.
3. Varnostne dogodke je potrebno razlikovati po stopnji nevarnosti.
4. Glede na stopnjo nevarnosti je vsakič obveščeno vodstvo letališke uprave, ki določa akterje za posamezno stopnjo nevarnosti obravnavanega dogodka.
5. Opustitev prijave varnostnega dogodka mora biti obravnavana kot disciplinski prestopek.
6. Odziv na varnostni dogodek mora biti kar se da hiter, da bi se s tem zmanjšalo možnost nadaljnjih dogodkov, ki bi škodovali sistemu.

## 3 Zaključek

Z uporabo navodil, ki jih zaposleni dobijo od vodstvenega kadra, ki se navezujejo na temeljne usmeritve s strani informacijsko varnostne politike, lahko letališča veliko naredijo na področju varnosti, ki bi morala biti vseskozi na visokem nivoju. Tako se morajo postaviti omejitve zaposlenim glede neopravičene uporabe ali zlorabe informacijsko komunikacijskih tehnologij, s katerimi bi morda namenoma ali ne namenoma lahko ogrozili ali škodovali informacijski varnosti znotraj letališča. Seveda pa mora vodstveni kader sam upoštevati ter spoštovati, predvsem pa zaposlene obveščati o varnostni politiki letališča ter novostih na tem področju. Ni torej dovolj le nalaganje obveznosti ter prepovedovanje določenih dejanj, bistveno je izvajanje informacijsko varnostne politike. Z izjavo o varovanju podatkov se zaposleni tako obvežejo molčečnosti glede temeljnih podatkov in informacij, s katerimi se srečajo v okviru službenih dolžnosti. Tudi po prenehanju delovnega razmerja se zaposleni ne smejo izpovedati o takšnih podatkih, ki lahko škodijo varnosti letališča.

## 4 Literatura


Dimc, M. (2009). Kriminaliteta v informacijski družbi. *Uporabna informatika, 17(2), 101-105*.

Informationsecurity forum. (2003). *The standard of good practice for information security*. Pridobljeno 25.3. 2011 na http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf

Ministrstvo za javno upravo. (2010). *Priporočila informacijske varnostne politike javne uprave*. Pridobljeno 15.5. 2011 na http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DEUP/IVPJU.doc_01.pdf

Stallings, W. in Brown, L. (2008). *Computer security: principles and practice*. New Jersey, Pearson Education.