**10. RIZICI PRIMJENE INFORMACIJSKE TEHNOLOGIJE U POSLOVANJU**

**10.1 ZLOPORABE INFORMACIJSKE TEHNOLOGIJE I INFORMACIJSKI RIZICI**

**Do zloporabe dolazi:**

* zbog ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina
* zbog nanošenja materijalne ili nematerijalne štete pojedincu, skupini ili zajednici

**Rizik→**opasnost da će poduzeta aktivnost dovesto do neželjenih posljedica

**Rizik informacijske tehnologije→**opasnost da bi njena primjena mogla dovesti do neželjenih posljedica za pojednica, u organizacijskom sustavu i/ili njegovoj dokolici

**Obilježja rizika:**

* težina
* učestalost

**Težina rizika→**mjerilo veličine štete što je određena aktivnost može izazvati i obično se može procijeniti i iskazati u financijskom obliku

**Učestalost (frekvencija) rizika→**procijenjeni broj poduzimanja potencijalno štetnih aktivnosti u jednici vremena

**Ovisno o uzroku, rizici mogu biti:**

* **objektivni→**proizlaze iz prirode i zakonitosti funkcioniranja sustava u kojem se informacijska tehnologija primjenjuje
* **subjektivni→**nastaju namjerom pojedinaca ili skupina, ili kad se u sustavu ne poduzimaju raspoložive mjere zaštite od objektivnih rizika

**Načela upravljanja rizicima:**

* treba omogućiti prepoznavanje svih rizika
* treba uspostaviti i dosljedno primjenjivati sustavne procedure procjene težine i frekvencije svih rizika
* treba razviti strategiju sustavnog praćenja i kontrole nad rizicima te izbora odgovarajućih zaštitinih mjera

**10.2. SIGURNOST INFORMACIJSKIH SUSTAVA I ZAŠTITA OD ZLOPORABA INFORMACIJSKE TEHNOLOGIJE**

**Sustav zaštite od zloporabe informacijske tehnologije obuhvača 3 oblika zaštite:**

1. zaštita informacijskog sustava od pristupa neovlaštenih osoba
2. zaštita zloćudnog koda
3. zaštita tajnosti podataka

**Zaštita informacijskog sustava od pristupa neovlaštenih osoba-mjere:**

* mjere fizičke zaštite
* mjere logičke zaštite

**Mjere fizičke zaštite→**klasične mjere koje se ostvaruju postavljanjem fizičkih prepreka pristupu materijalnim elementima informacijskog sustava ili angažiranjem zaštitarske službe

**Mjere logičke zaštite→**ostvaruju se primjenom računala i odgovarajućih programa, a mogu se ostvariti na dva načina:

* kao fizička identifikacija korisnika
* kao logička identifikacija korisnika

**Fizička identifikacija→**pretpostavlja da korisnik posjeduje neki predmet ili ima neku biološku osobinu što ga jednoznačno razlikuje od svih ostalih potencijalnih korisnika

**Logička identifikacija→**zasniva se na provjeri zna li korisnik nešto što bi trebao znati odnosno da li može saznati bez činjenja prekršaja

* lozinka
* ključ
* identifikacijski ključ
* osobni identifikacijski broj
* ključna riječ

**Sustavi korisničkih ovlasti njihove provjere:**

* slojeviti
* selektivni

**Biometrijske metode→**polazi od pretpostavke da ljudi imaju neka jednistvena biometrijska obilježja

**2 tipa biometrijskih karakteristika:**

* fizičke osobine gdje se proces identifikacije temelji na otisku prsta, otisku i geometriji šake, geometriji lica, karakteristikama šarenice i mrežnice oka
* osobine ponašanja pojedinaca gdje se identifikacija obavlja pomoću govora, rukopisa, kretnji pri hodanju, tipkanju po tastaturi

**Proces identifikacije/verifikacije:**

1. uzimanje identificirajućeg (prvog) otiska
2. pohranjivanje u bazu podataka
3. identifikacija
4. verifikacija uzetog i pohranjenog otiska
5. odobravanje ili uskraćivanje obavljanja daljnjinh postupaka

**2 temeljna načina pretraživanja pohranjenih zapisa:**

* jedan prema više
* jedan prema jedan

**Pouzdanost metode identifikacije može se analizirati sa dva aspekta:**

1. aspekt korisnika u smislu postojanosti biometrijskih karakteristika pojedinaca
2. aspekt tehnologije u smislu pouzdanosti uređaja, tj. same metode uzimanja otisaka

**Točnost prepoznavanja u procesu identifikacije; tri načina mjerenja:**

* prvi način mjerenja iskazuje broj pogrešno prihvačenih pokušaja identifikacije
* drugi način mjerenja iskazuje broj pogrešno odbijenih pokušaja identifikacije
* treći način mjerenja iskazuje broj bezuspješnih pokušaja identifikacije zbog neodgovarajućeg identicifirajućeg otiska

**Višestruka identifikacija→**proces identifikacije u kojem se osoba identificira s više nego jednom identificirajućom karakteristikom, tj. više nego jednom metodom identifikacije

**Višestruka biometrijska identifikacija→**proces identifikacije u kojem se kombiniraju metode identifikacije temeljene na fizičkim osobinama pojedinca međusobno ili u kombinaciji s metodama utemeljenima na osobinama ponašanja

**4 scenarija u kojem se skupljaju podaci kako bi se formirao uzorak:**

1. jedna biometrijska osobina, više skenera
2. jedna biometrijska osobina, jedan skener
3. jedna biometrijska osobina, više jedinki
4. više biometrijskih osobina

**Fuzija uzoraka moguća je na tri različita mjesta u procesu identifikacije:**

1. u modulu ekstrakcije biometrijskih osobina
2. u modulu uparivanja
3. u modulu odluke

**Zaštita od zloćudnog koda**

**Računalni virusi→**računalni programi ili dijelovi programskog koda koji su unijeti u računalo i izvode se bez znanja i dopuštenja vlasnika računala

**Zloćudni kod→**programi oblikovani s ciljem da se infiltriraju u računalne sustave i načine neku vrstu štete. Podjela:

* mrežni crvi→sami sebe kopiraju, šalju u računalnu mrežu, te napadaju ostala računala u mreži
* trojanski konji→stvaraju privid da obavljaju neke dopuštene računalne operacije, a zaparvo čine nešto drugo, najčešće štetno
* špijunski programi→nedopušteno prate aktivnosti korisnika računala, evidentiraju ih, i te informacije šalju nekim neovlaštenim osobama
* neovlašteni reklamni (oglasni) softver→korisnika računala „bombardira“ i uznemirava reklamnim porukama, iako nije dobio dopuštenje
* softver za financijski kriminal→bez dopuštenja i znanja korisnika obavlja neke neželjene i štetne financijske transakcije

**Mjere zaštite od zloćudnog koda:**

* preventivne→“bolje spriječiti nego liječiti“
* kurativne→liječenje

**Problem sa idejom zaštite tajnosti podataka se nastoji rješiti na dva načina:**

1. poduzimanjem mjera ograničavanja dostupnosti podataka i elemenata informacijskih sustava
2. poduzimanjem mjera ostvarivanja prividne nerazumljivosti

**Kriptografske metode zaštite podataka**

**Kriptologija→**znanost o prikrivanju stvarnohg informacijskog sadržaja izgovorenih ili napisanih poruka

**Podjela:**

* **kriptografija→**znanost o metodama ostvarivanja nerazumljivosti porukaod strane onih subjekata kojima nisu upućene
* **kriptoanaliza→**znanost o ostvarivanju razumljivosti poruka, prethodno kriptografiranih, od strane subjekata koji su ih primili, a da to nisu trebali

**Otvoreni tekst→**oblik u kojemu je iskazana izvorna poruka, a nakon primjene neke kriptografske metode naziva se **kriptogram ili šifrat**

**Osnovne skupine kriptografskih metoda:**

* metoda premještanja→postupci u kojima se kriptogram stvara zamjenom mjesta znakova otvorenog teksta
* metoda zamjene→znakovi izvorne poruke su napisani u jednoj izvornoj abacedi, znakovima neke druge kodne abecede

**Enkripcija→**metoda zamjene u kojemu je kodna abeceda zapravo neki brojevni sustav

**Kriptološki algoritmi→**mješavina većeg broja metoda premještanja i metoda supstitucije, a postupak stvaranja kriptograma odvija se u većem broju slijednih ili ponavljajućih koraka

**10.3. PROBLEMI SIGURNOSTI U ELEKTRONIČKOM POSLOVANJU I INFORMATIČKI KRIMINALITET**

**Informatički kriminalitet→**ukupnost protupravnih aktivnosti pri kojima infomacijska tehnologija služi kao sredstvo činjenja ili objekt napada

**Osnovne kategorija kriminalnih aktivnosti:**

1. napadi na resurse tvrtke
2. napadi na privatnost i krađa identiteta
3. ugrožavanje integriteta podataka
4. ometanje normalnog rada i poslovanja