Rizici primjene informacijske tehnologije u poslovanju

Sadržaj predavanja

 Etika i informacijska tehnologija

 Rizik informacijske tehnologije

 Informatički kriminalitet

 Metode zaštite

 Problemi sigurnosti u e-poslovanju

Etika i informacijska tehnologija

 Informacijska se tehnologija može koristiti na dobrobit pojedinca, društvenih skupina i poslovnih organizacija, ali njena primjena može rezultirati i negativnim učincima,

izazvanima slučajno, iz neznanja ili nemara, ili pak namjerno.

 Korištenje IT zato valja urediti odgovarajućom pravnom regulativom, no važno je pridržavati se i određenih etičkih načela.

Osnovna etička načela primjene IT postavio je još 1992. godine Institut za računalnu etiku

(Computer Ethics Institute):

Nitko ne bi smio korištenjem IT nanositi štetu, bol ili neugodu ostalim ljudima.

Nitko ne bi smio korištenjem IT ometati druge ljude u korištenju te tehnologije.

Nitko ne bi smio „kopati“ po tuđim podacima odnosno informacijama bez znanja i privole njihova vlasnika.

Nitko ne bi smio koristiti IT radi krađe.

Nitko ne bi smio koristiti IT radi prikrivanja stvarnih dokaza ili stvaranja lažnih dokaza.

Softver čiji je vlasnik poznat ne bi se smio koristiti bez plaćanja novčane naknade koju za to traži vlasnik.

Nitko ne bi smio svojatati ili prisvajati tuđe intelektualno vlasništvo.

Svatko treba uvijek koristiti IT tako da njome ne ugrožava okolinu i druge osobe i da poštuje prava svojih suradnika i drugih osoba.

Zlouporabe IT u poslovanju

 Do zlouporabe IT može doći iz dva razloga:

radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih

skupina

radi namjernog nanošenja materijalne ili nematerijalne štete pojedincu ili organizaciji

 U oba slučaja uporaba tehnologije predstavlja kršenje pravnih i/ili moralnih normi i podložna je sankcijama.

Rizik informacijske tehnologije

 Rizik informacijske tehnologije predstavlja opasnost da njezina primjena dovede do

neželjenih posljedica

 Vrste rizika:

◦ Objektivni – prirodni (požar, poplava, prašina) i posljedica ljudske nenamjerne pogreške

(brisanje podataka, pogrešno rukovanje)

◦ Subjektivni – nastaju kao posljedica ljudske namjerne aktivnost

Najvažniji primjeri subjektivnih rizika (1)

 Zloupotreba ovlaštenja

 Službenik banke prebacuje novac sa računa klijenta na svoj račun

 Neodgovarajuća razdioba ovlaštenja

 Programer umjesto knjigovođe korigira bilancu

 Neodgovarajuća kontrola

 Blagajnik evidentira isplatu koju nije izvršio, bez znanja kontrolora

Najvažniji primjeri subjektivnih rizika (2)

 Nedostatak kontrole nad mogućim promjenama u računalnim programima

◦ Programer modificira program tako da sebi poveća plaću

 Zloupotrebe za koje trebaju posebno znanje

◦ Lažiranje rezultata u igri na sreću u kojoj se dobici izvlače pomoću računala

 Korištenje izuzetnih prilika u poslovnom sustavu

◦ Skladištar evidentira lažne podatke o veličini nastalih šteta zbog požara iako su štete bile zanemarive

Informatički kriminalitet

 Vrste:

◦ 1. Manipulacija sredstvima informacijske tehnologije

◦ 2. Neovlaštena upotreba softvera i povreda vlasništva

◦ 3. Sabotaže

◦ 4. Virusi

◦ 5. Zloporaba Facebook računa

◦ 6. Zloporaba bankomata, inteligentnih kartica i slično

◦ 7. Zloupotreba privatnosti

Primjeri manipulacije sredstvima IT-a

 Namjerno pogrešno obračunat porez

 Namjerno uvođenje lozinki koje imaju veća ovlaštenja nego što je predviđeno

 Namjerno slanje e-mail poruke na pogrešnu adresu

 Krađa CD-a, disketa…

 Probijanje tuđih lozinki, lažno predstavljanje

 Phishing – lažna web mjesta

Socijalni inženjering

 Socijalni inženjering je manipulacija ljudima (prijevara) u svrhu otkrivanja povjerljivih informacija.

 Napadači na neki način pokušavaju biti uvjerljivi. Tako npr. u e-mailu navode neki poznati podatak o korisniku (npr. ime koje može biti poznato jednostavno iz e-mail adrese), datum rođenja itd.

 Napadači se obično uzdaju u zakon velikih brojeva i šire velike količine poruka (spam) kako bi putem socijalnog inženjeringa navukli djelić korisnika da učine ono što

žele.

 Phishing je jedan od oblika socijalnog inženjeringa u kojem napadači pokušavaju dođi do brojeva kreditnih kartica, lozinki različitih korisničkih računa i sl.

Primjeri neovlaštene upotrebe softvera

 Kopiranje programa od strane krajnjih korisnika

 Kopiranje programa sa “razbijenim” sustavima zaštite – sa Interneta i od korisnika

 Krivotvorenje programa

 Neovlašteno iznajmljivanje

Primjeri sabotaža

 Ručne sabotaže – brisanje programa

 Stvaranje nenormalnih uvjeta rada – strujni udar, vlaga, toplina

 Hakeri – neovlašten pristup računalima, ali ne mora uvijek biti zbog koristi i nanošenja štete

Računalni virusi

 dijelovi programa koji se komunikacijom ili putem memorijskih medija unose u računalni sustav

 pridodaju se u postojeće programe i djeluju pri njihovom pokretanju

mrežni crvi (engl. Network Worm, Worm) - sami sebe kopiraju i šalju u računalnu mrežu

te „napadaju“ ostala računala u mreži

trojanski konji (engl. Trojan Horse, Trojan) – stvaraju privid da obavljaju neke dopuštene računalne operacije, dok u stvari čine nešto sasvim drugo, obično štetno po računalo i/ili u njemu pohranjene podatke

špijunski programi (engl. Spyware) - nedopušteno prate aktivnosti korisnika računala, evidentiraju ih i informacije o tome šalju neovlaštenim osobama ili

organizacijama

neovlašteni reklamni (oglasni) softver (engl. Advertising Software, Adware) - korisnika računala uznemiruju reklamnim porukama bez korisnikova dopuštenja

Zloupotreba Facebook računa











Zloupotreba bankomata

 Postavljaju se minijaturna kamera i čitač koda koji omogućuju iščitavanje i prenošenje svih

podataka s originalne kartice na vjernu kopiju

 Sa kopijom se može podizati novac i plaćati usluge kao s "pravom" karticom

Zloupotreba privatnosti

 Podaci korisnika

 Spam

 Kontrola korištenja Interneta na poslu

 Čitanje tuđe elektronske pošte

 Nadziranje navika i interesa pojedinaca

◦ Spyware, kolačići

Metode zaštite

Sigurnost informacijskih sustava

 Neophodno je razviti odgovarajući sustav zaštite od zlouporabe IT.

Takav sustav mora obuhvaćati tri oblika zaštite:

a) zaštitu IS-a od pristupa neovlaštenih osoba

b) zaštitu od zloćudnog koda

c) zaštitu tajnosti podataka (informacijskog sadržaja)

Nije dovoljno uspostaviti samo neki ili neke već obvezno sve navedene oblike zaštite od zloporabe IT.

a)

 U svrhu zaštite IS-a od informacijskih rizika primjenjuju se dvije osnovne skupine mjera:

mjere fizičke zaštite – postavljanje fizičkih prepreka pristupu materijalnim elementima

informacijskog sustava (zaključavanje prostorija, postavljanje ograda, itd.) ili angažiranje zaštitarske službe

mjere logičke zaštite - identifikacija korisnika i provjera ovlaštenosti (autoriziranosti) korisnika za uporabu resursa IS-a

Identifikacija korisnika

 Postupak identifikacije korisnika znači provjeru je li korisnik zaista ona osoba kojom se

predstavlja računalu (IS-u).

 Može se ostvariti na dva načina:

fizičkom identifikacijom korisnika

logičkom identifikacijom korisnika

Fizička identifikacija korisnika

 Fizička identifikacija pretpostavlja da korisnik:

posjeduje neki predmet (npr., identifikacijsku karticu s kodiranim podacima potrebnima za provjeru identiteta, neki oblik materijalnog ključa za aktiviranje određenog uređaja, itd.), ili

ima neku biološku osobinu (npr. otisak prsta, glas, sliku očne šarenice, DNK karakteristiku) što ga jednoznačno razlikuje od svih ostalih potencijalnih korisnika.

 U svrhu fizičke identifikacije korisnika sve se češće primjenjuju biometrijske metode.

Biometrijske metode indentifikacije

 Razvijaju se u okrilju biometrije, znanstvene discipline koja se bavi izučavanjem i mjerenjem jedinstvenih bioloških karakteristika čovjeka.

 Razlikuju se dva tipa biometrijskih karakteristika:

fizičke osobine pojedinca (otisak prsta, otisak i geometrija šake, geometrija lica, karakteristike šarenice i mrežnice oka, geometrija uha, DNA)

osobine ponašanja pojedinca (govor, rukopis, kretnje pri hodanju, korištenje tipkovnice)

Logička identifikacija korisnika

 Zasniva se na provjeri zna li korisnik nešto što bi trebao znati.

 Podatak kojega bi korisnik trebao znati naziva se općenito lozinkom ili zaporkom (engl. Password), a u nekim slučajevima rabe se i nazivi kao što su: ključ (engl. Key), identifikacijski ključ (engl. Identification Key, ID, User ID), osobni identifikacijski broj (engl. Personal Identification Number, PIN), korisničko ime (engl. User Name), ključna riječ (engl. Keyword), itd.

b)

Zaštita od zloćudnog koda

 Popularno se naziva i antivirusnom zaštitom, što nije sasvim korektno, jer su računalni virusi samo jedan od brojnih oblika zloćudnog koda.

 Općenito, zloćudni kod (engl. Malicious Software, Malware) su računalni programi oblikovani s ciljem da se infiltriraju u računalne sustave i načine neku

vrstu štete.

 Računalni virusi se samostalno razmnožavaju

 Primjenjuju se dvije skupine mjera zaštite od zloćudnog koda (po ugledu na mjere zaštite od bioloških virusa):

mjere preventivne zaštite – “bolje spriječiti, nego liječiti"

mjere naknadne zaštite – ako do zaraze ipak dođe, treba primijeniti odgovarajuće “lijekove”

 Nikakve mjere zaštite od zloćudnog koda nisu apsolutno pouzdane – postoje samo bolje i lošije.

c)

 Zaštita tajnosti podataka nastoji se ostvariti poduzimanjem mjera:

ograničavanja dostupnosti podataka i ostalih elemenata IS-a – fizička i logička zaštita IS-a

ostvarivanja prividne nerazumljivosti inače dostupnih podataka od strane neovlaštenih

korisnika – kriptografske metode zaštite podataka

Kriptografske metode zaštite podataka

 Kriptologija (grč. krypto = skriven, logos = govor) je znanost o prikrivanju stvarnog informacijskog sadržaja izgovorenih ili napisanih poruka.

 Dijeli se na:

kriptografiju, kao znanost o metodama ostvarivanja nerazumljivosti poruka za one kojima poruke nisu upućene, i

kriptoanalizu, kao znanost o ostvarivanju razumljivosti kriptiranih poruka od strane onih koji su ih primili a da to nisu smjeli.

 Oblik u kojemu je iskazana izvorna poruka naziva se otvoreni tekst, a nakon primjene neke

kriptografske metode oblik u kojemu će biti ta ista poruka naziva se kriptogram.

 Kriptografija se primjenjuje prilikom prijenosa podataka nezaštićenim računalnim

mrežama (npr., Internetom), ali i pri pohranjivanju osjetljivih podataka u računalnim memorijama.

Problemi sigurnosti u elektroničkom poslovanju

 Usporedo s razvitkom e-poslovanja razvija se i novi oblik kriminaliteta, tzv. informatički

kriminalitet.

 Pod tim se nazivom podrazumijeva ukupnost protupravnih aktivnosti pri kojima informacijska tehnologija služi kao sredstvo činjenja i/ili objekt napada.

 Prema procjenama američkog Federalnog istražnog ureda (FBI), zbog poteškoća pri

otkrivanju takvih protupravnih djela i komplikacija u dokaznom postupku tek jedan od tisuću vjerojatnih prekršitelja biva osuđen.

 Osnovne kategorije informatičkih kriminalnih aktivnosti su:

Napadi na resurse tvrtke – netko pokušava neovlašteno pristupiti fizičkim i/ili logičkim

resursima tvrtke

Napadi na privatnost i krađa identiteta – netko se lažno predstavlja, neovlašteno čita ili kopira podatke

Ugrožavanje integriteta podataka – netko nastoji smanjiti pouzdanost i vjerodostojnost informacija kako bi nanio štetu pojedincu ili organizaciji

Ometanje normalnoga rada i poslovanja – netko napada informatičke resurse tvrtke kako bi izazvao smanjenje kvalitete usluga koje tvrtka nastoji pružiti klijentima

Plan upravljanja rizicima

 1. Korak – Prepoznati rizike

◦ Odrediti moguće rizike u poduzeću

◦ Odrediti težinu i učestalost rizika

 2. Korak – Utvrditi prioritete poduzimanja protumjera ovisno o težini i učestalosti rizika

 3. Korak – Definirati moguće protumjere i analizirati odnos troška i dobiti

 4. Korak – Odabir i primjena protumjera

 5. Korak – Definiranje mjera otklanjanja već nastalih šteta

 6. Korak – Nadzor i modificiranje plana upravljanja rizicima