Varovanje informacij

E-izobraževanje Kreditni posredniki

NLB

Namen in cilj

Namen izobraževanja je kreditne posrednike seznaniti z osnovnimi načeli varovanja informacij v procesu odobravanja kreditov

NLB

Kaj je varovanje informacij?

Besedi informacija pripisujemo v vsakdanjem življenju, glede na kontekst v katerem nastopa, različne pomene in definicije (npr. informacije o voznem redu, informacijska družba, informacija o stanju na računu, informacija v računalniški obdelavi, ipd). Informacije se nahajajo na / v informacijskih sredstvih, ki so lahko v različnih oblikah: pisni dokument, človeški govor, digitalno zapisana računalniška datoteka, zapisana na spletu, video ali audio posnetek, biometrični zapis in podobno.

Vsekakor gre za vsebino, ki prejemniku nekaj novega pove in mu tako olajša odločanje.

Informacije obravnavamo kot **premoženje podjetja**. Zavedati se moramo poslovne škode, ki bi jo utrpelo podjetje ob izgubi, nepooblaščenemu razkritju ali nepravilni informaciji, izraženo v višini morebitnih tožb, kot izgubo deleža trga ali izgubo ugleda podjetja v okolju.

Varovanje informacij pomeni zagotavljanje 3 bistvenih lastnosti informacij:

- **Zaupnost**: Informacije so dostopne samo tistim, ki so za to pooblaščeni;
- **Celovitost**: Varovanje točnosti in popolnosti informacij in informacijskih sistemov;
- **Razpoložljivost**: Pooblaščeni uporabniki imajo dostop do informacij takrat, ko jih potrebujejo.

Kaj je potrebno varovati?

Varovanje informacij ne obsega le informacij samih, ampak tudi vsa ostala sredstva, ki omogočajo uporabo informacij:

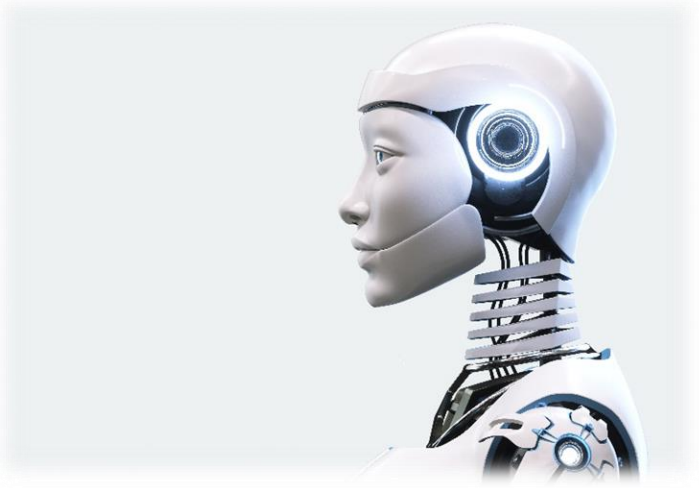
Informacije
– podatkovne zbirke in datoteke s podatki
– sistemska dokumentacija, operativni in podporni postopki, uporabniški priročniki, načrti za neprekinjeno delovanje,…
– projektna dokumentacija, delovni postopki, uporabniška navodila,…
– pogodbe, naročila,… (podatki o komitentih in poslih)
– poročila o poslovanju

Programska oprema
– aplikacijska programska oprema
– sistemska programska oprema
– razvojna orodja in podporni programi

Storitve
– računalniške in komunikacijske storitve
– druge tehnične storitve (razsvetljava, električno napajanje, klima)

Ljudje
– zaposleni, pogodbeniki, zainteresirane stranke

Fizična sredstva
– računalniška in komunikacijska oprema
– nosilci podatkov (diski, trakovi, CD-ROM, ključki, ...)
– druga tehnična oprema (naprave neprekinjenega delovanja – UPS napajalniki, hladilne naprave)
– prostori, pohištvo



NLB

Primeri varnostnih incidentov v Sloveniji

Vdor v elektronsko pošto ministrice Klampferjeve: malomarnost ali namerna napaka?
Pri sumu kaznivega dejanja vdora v elektronsko pošto ministrice za delo Ksenije Klampfer gre najverjetneje za hudo malomarnost ali pa namerno napako računalniškega administratorja. Zaradi tega so v njeno službeno elektronsko pošto lahko le z nekaj kliki nepooblaščeno dostopali številni uslužbenci ministrstva.

Lekarna Ljubljana je bila v avgustu 2019 tarča napada z izsiljevalskim virusom, ki je vplival na razpoložljivost informacij in informacijskega sistema. Nepridipravom je uspelo zakleniti celotno bazo podatkov. Poslovalnice so bile zaprte, šele zvečer so izdajanje na papirnati recept vzpostavili v enoti pri polikliniki, naslednji dan so obnovili izdajo zdravil na papirnati recept.
Vir: 24ur.com

Intersport tarča hekerskega napada: skušali skenirati podatke o kreditnih karticah
Tarča zlonamernega napada so bile slovenska, hrvaška, srbska, bosanska in makedonska spletna stran. V hekerskem napadu so na spletno stran namestili kodo, ki naj bi domnevno skenirala podatke o kreditnih karticah, vendar po podrobnem preverjanju do omenjene aktivnosti ni prišlo, kodo pa so odstranili.
Vir: 24ur.com

Osnovni ukrepi, ki jih zagotavlja posameznik – kreditni posrednik 1/2

Varovanje informacij je sestavljeno iz ukrepov in postopkov, ki jih opravimo zaposleni z namenom, da informacije zaščitimo pred odtujitvijo, zlorabami, uničenjem, poškodovanjem oziroma kakšnim drugim, za podjetje škodljivim dejanjem.

Pri tem uporabljamo znanje, psihofizične sposobnosti, dokumentacijo, tehnična sredstva in opremo.

Varovanje informacij obsega logične, organizacijske in tehnične postopke in ukrepe za varovanje v vseh fazah življenjskega cikla informacij. To pomeni tako v fazi nastajanja, obdelovanja, prenašanja, hranjenja, arhiviranja, kot tudi uničevanja informacij.

NLB

Osnovni ukrepi, ki jih zagotavlja posameznik – kreditni posrednik 2/2

Osnovni ukrepi, ki jih zagotavlja kreditni posrednik

Določilo "čista miza" pomeni, da moramo zaposleni, v času odsotnosti s svojega delovnega mesta, vse informacije, ki niso za javno objavo pospraviti v predal ali omaro. Na ta način preprečimo, da bi se nepooblaščena oseba seznanila s podatki oziroma informacijami.

Določilo "čisti ekran" pomeni, da moramo vsakokrat, preden zapustimo vklopljeno delovno postajo, leto ročno zakleniti. To naredimo s pritiskom tipk "Ctrl+Alt+Delete" in potrditvijo izbora "Lock this Computer". Tako preprečimo nekomu drugemu uporabo delovne postaje, ki je prijavljena v sistem pod uporabniku lastnim imenom in geslom. Hkrati preprečimo tudi branje informacij z ekrana.

Načelo »need to know« pomeni, da so podatki na razpolago le osebam, ki jih potrebujejo za realizacijo svojih delovnih zadolžitev.

Zagotavljanje zaupnosti podatkov pomeni, da podatke in informacije, ki smo jih pridobili v okviru procesa odobravanja NLB Kredita na prodajnih mestih ne delimo s posamezniki, ki niso upravičeni do seznanitve s tovrstnimi podatki oziroma informacijami.

Prepovedano posojanje uporabniških imen in gesel oziroma drugih komponent na katere kreditni posrednik prejema geslo (enkratno geslo) za dostop do aplikativne podpore NLB Krediti na prodajnih mestih. Uporabniško ime in geslo služita za preverjanje identitete uporabnika in evidentiranje dostopa uporabnika do podatkov. Uporabniki se moramo zavedati, da smo osebno odgovorni za vse akcije in transakcije, ki so vezane na naše uporabniško ime in geslo. Vsak dostop do aplikativne podpore NLB Krediti na prodajnih mestih kot tudi aktivnosti, ki jih uporabnik realizira pri uporabi aplikativne podpore, se beležijo v t.i. revizijski sledi.

Neobičajno delovanje aplikativne podpore NLB Krediti na prodajnih mestih smo dolžni nemudoma javiti kontaktni osebi pri kreditnem posredniku, ki mora nemudoma poročati naprej NLB.

NLB

Zaključek

Namen varovanja informacij je PREPREČEVATI s ciljem OHRANJATI zaupnost / celovitost / razpoložljivost podatkov in informacij.

Z varovanjem informacij **preprečujemo**:

- nezakonito, neupravičeno in nepooblaščeno poseganje v informacije,
- nastanek večje poslovne škode,
- realizacijo operativnih tveganj (npr. prekinitev delovanja informacijskega sistema).

Z varovanjem informacij **ohranjamo**:

- zaupnost - dostopnost do informacij le pooblaščenim osebam,
- celovitost - pravilnost in popolnost podatkov in obdelav,
- razpoložljivost - podatki in obdelave so dostopne uporabnikom, ko jih potrebujejo.

Varovanje informacij je del etičnega ravnanja in vrednota vsakega zaposlenega. Za izvajanje varovanja informacij in za skrbnost varovanja informacij smo odgovorni vsi zaposleni.

NLB