VARNOST SPLETNIH STORITEV UJP

V Upravi Republike Slovenije za javna plačila nenehno skrbimo za varnost svojih spletnih storitev. Prvi nivo varnosti je zagotovljen z uporabo šifrirane povezave in digitalnih potrdil. Drugi nivo je zagotovljen z uporabo gesla in sistema uporabniških pravic.

Priporočamo uporabo digitalnih potrdil na t.i. pametni kartici, na kateri je natisnjeno ime lastnika, v samem zapisu na pametni kartici pa so zapisani podatki o lastniku v obliki kvalificiranega digitalnega potrdila po standardih PKI. Če pametno kartico izgubite in jo nepošteni najditelj poskuša uporabiti, se kartica zaklene po treh poskusih vpisa napačne osebne številke, da nadaljnja uporaba ni več mogoča.

Uprava Republike Slovenije za javna plačila
Dunajska cesta 48, 1000 Ljubljana

Telefon: (01) 4751-651

E-pošta: ujp@ujp.gov.si

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA FINANCE
UPRAVA REPUBLIKE SLOVENIJE ZA JAVNA PLAČILA

Spletna varnost

V Upravi Republike Slovenije za javna plačila smo usmerjeni v odličnost izvajanja storitev, informatizacijo in avtomatizacijo procesov, širjenje elektronske izmenjave podatkov in plačil ter profesionalen razvoj zaposlenih.

Ukrepi na področju spletne varnosti

Gesla in dostopi

Uporaba spletnih storitev je najpogosteje zavarovana z uporabniškim imenom in geslom.

Napotki:

- izberite dolga gesla, sestavljena iz črk, številk in posebnih znakov, v geslih ne uporabljajte svojih osebnih podatkov in podatkov o svojih bližnjih (imena otrok, ljubljenčkov, rojstnih datumov ipd.),

- če je le možno, si gesla zapomnite,

- uporabniških imen in gesel ne posojajte nikomur,

- pred vpisom uporabniškega imena in gesla v spletni obrazec, se prepričajte, ali ste res na pravi strani ter ali je v naslovu "https",

- ob nameščanju mobilnih aplikacij privzeto ne potrjujte vseh zahtev za delitev stikov in ostalih podatkov, saj jih lahko ta aplikacija ne potrebuje za svoje delovanje.

Digitalna potrdila

Eden od varnostnih mehanizmov spletnih storitev UJP so digitalna potrdila.

Napotki:

- pametne kartice ali USB ključka z digitalnim potrdilom med odsotnostjo ne puščajte v računalniku, temveč ju izvlecite in shranite na varnem mestu,

- digitalnega potrdila nikoli ne posojajte sodelavcem,

- ob prenehanju uporabe službenega digitalnega potrdila, se z delodajalcem dogovorite o načinu preklica digitalnega potrdila,

- redno menjajte PIN kodo na pametni kartici,

- nosilca digitalnega potrdila nikoli ne hranite skupaj z gesli ali PIN kodo.

Izobraževanje

Pri krepitvi spletne varnosti je pomembno izobraževanje uporabnikov, kar se lahko izvaja preko delavnic, spletnih učilnic in obiskov raznih dogodkov.

Mesec oktober je mesec spletne varnosti, ko se v številnih državah odvijajo aktivnosti ozaveščanja o spletni varnosti.

Več o tem: https://cybersecuritymonth.eu/

V Sloveniji se pod okriljem ARNES izvaja projekt Varni na internetu, ki je dosegljiv na spletni strani

https://www.varninainternetu.si/

Elektronska pošta

Obseg elektronske pošte s škodljivo kodo in škodljivimi povezavami se vsako leto povečuje.

Napotki:

- ne odpirajte elektronske pošte, priponk ter povezav od neznanih pošiljateljev,

- nikoli nikomur ne pošiljajte občutljivih podatkov (gesla, digitalna potrdila ipd.),

- zlonamerna pošta od nas zahteva takojšnja dejanja, je pospremljena z neknjižnim jezikom in pogosto z besedami, kot so: nemudoma, takoj, urgentno, opozorilo,

- UJP od vas nikoli ne zahteva pošiljanja občutljivih podatkov preko elektronske pošte.

Sistemski ukrepi

V organizaciji naj se vzpostavijo in izvajajo sistemski ukrepi za višanje nivoja informacijske varnosti:

- politika čiste mize,

- politika najmanjših pravic,

- politika dostopa do informacijskih virov,

- politika dostopa do omrežja,

- politika upravljanja in varovanja gesel,

- varnostna politika za zunanje izvajalce in obiskovalce itd.

Brezžična omrežja

Brezžično omrežje lahko danes vzpostavi kdorkoli in kadarkoli. Najvarneje je predpostavljati, da nobeno javno brezžično omrežje ni povsem varno.

To velja tudi za velika omrežja, kot so npr. knjižnice, letališča, ipd., saj se tam zadržuje veliko število napadalcem zanimivih ljudi.

Napotki:

- na napravah izključite samodejno povezavo na brezžična omrežja,

- izključite skupno rabo datotek,

- če je za vstop v omrežje predvideno soglašanje s pogoji poslovanja, jih skrbno preberite,

- vsi nekriptirani podatki (gesla, elektronska pošta), izmenjani preko omrežja se lahko opazujejo in shranjujejo v nepoštene namene,

- uporabljajte varno ("https") povezavo,

- uporabljajte posodobljeno programsko opremo,

- vključite požarni zid in posodobljeno protivirusno zaščito,

- če je možno, uporabite zasebno navidezno omrežje (VPN), ki šifrira promet po omrežju.