DEŽELNA BANKA SLOVENIJE

DBS NET

Varnost poslovanja

Sektor plačilnega prometa

Ljubljana, junij 2020

1 Varnost na strani elektronske banke

V elektronsko banko smo vgradili več varnostnih mehanizmov, ki so rezultat najsodobnejše tehnologije za zaščito podatkov in transakcij prek omrežja internet. S tem je zagotovljena varna uporaba vseh storitev, ki jih nudi ta sodoben način poslovanja. Elementi omenjene večstopenjske zaščite so:

1. požarna pregrada,
2. šifriranje podatkov na svetovnem spletu,
3. šifriranje podatkov elektronske pošte,
4. varna prijava v elektronsko banko,
5. varnostni sistem proti ugibanju gesla,
6. varnostni sistem samodejne odjave,
7. varnostni sistem ugotavljanja in dodatnega potrjevanja neobičajnih transakcij.

1.1 Požarna pregrada

Požarna pregrada (ang. Firewall) je varnostni programski sklop, ki loči zunanji del računalniškega omrežja od notranjega dela omrežja banke ter onemogoča nepooblaščenim dostop do podatkov. Deluje tako, da nadzoruje in spremlja vse vhodne podatke v omrežje banke, pri čemer preverja njihove vire in cilje, beleži nepravilne poizkuse in zavrnjene dostope do omrežja ter tako skrbi, da so notranji naslovi zaščiteni pred zunanjimi vdori. Na ta način so zaščiteni tudi strežniki, ki so namenjeni delovanju DBS NET in DBS PRONET.

1.2 Šifriranje podatkov na svetovnem spletu

Celotna komunikacija med spletnim brskalnikom, ki ga uporabnik uporablja za dostop do elektronske banke in strežnikom banke poteka z uporabo t.i. Transport Layer Security protokola (TLS protokola). ***TLS protokol*** je množica pravil za šifriranje sporočil, ki potekajo v obeh smereh, in je vgrajen v večino brskalnikov, ki so vsakodnevno uporabljeni. Uporaba šifriranih sporočil (kriptografija) je eden izmed najpomembnejših načinov zagotavljanja varnosti v računalniških omrežjih, saj se s tem informacije spremeni v obliko, ki onemogoča njihovo razumevanje. **Šifrirana podatkovna linija vam tako v celoti zagotavlja zasebnost komunikacije, ki jo imate z banko in onemogoča prisluškovanje na vmesnih komunikacijskih točkah**.

Zaščita sporočil je odvisna od velikosti šifrirnega ključa. V Deželni Banki Slovenije d.d. uporabljamo ključ velikosti 2048 bitov, ki zagotavlja najvišjo možno stopnjo varnosti.

Ustreznost vzpostavljene šifrirane povezave lahko vselej preverite v naslovni vrstici brskalnika, kjer je naveden naslov spletnega mesta (URL povezave) na katerem se nahajate. V vseh sodobnih spletnih brskalnikih ustreznost šifrirane povezave predstavlja ikona zaklenjene ključavnice in oznaka HTTPS (ang. Hypertext Transfer Protocol Secure). S klikom na ikono ključavnico lahko preverite tudi izdajatelja digitalnega potrdila in njegovo veljavnost.

V kolikor imate v naslovni vrstici brskalnika prepolovljeno ključavnico ali ključavnice ni, oziroma, če je pred naslovom spletnega mesta oznaka HTTP, sporočila niso šifrirana! To lahko pomeni, da so bile spremenjene nastavitve vašega brskalnika ali ste bili preusmerjeni na stran, ki ne pripada ponudniku varnih spletnih strani. V tem primeru obstaja visoko tveganja za prestrezanje podatkov in njihovo spreminjanje (ang. Man-in-the-Middle Attack).

V kolikor pri uporabi elektronske banke v vašem brskalniku opazite, da je ključavnica prepolovljena ali da ključavnice sploh ni, oziroma, da je pred naslovom spletnega mesta oznaka HTTP, nemudoma zapustite elektronsko banko, zaprite vsa okna brskalnika ter kontaktirajte banko.

1.3 Šifriranje podatkov, ki potekajo po elektronski pošti

Naročilo obveščanje o spremembi stanja na vaših računih, ki ga izvedete prek elektronske banke, poteka preko elektronske pošte brez šifriranja podatkov.

Za varno dvosmerno komunikacijo strank z banko uporabljamo šifrirana sporočila v sklopu elektronske banke. Obvestila delujejo podobno kot spletna pošta v brskalnikih, s tem da zagotavljajo enako visok nivo varnosti, kot velja za elektronsko banko.

Svetujemo vam, da za komunikacijo z banko izberete elektronsko banko namesto komunikacije preko elektronske pošte. V elektronski banki lahko sporočilo naslovite neposredno na vašega skrbnika s klikom na njegovo ime, lahko pa ga oddate preko reklamacijske številke ali preko rubrike 'Pripombe in mnenja'.

1.4 Varnost prijave v elektronsko banko

Ob poskusu prijave v elektronsko banko banka preveri vašo identiteto. To banka izvede na način, da opravi avtentikacijo (overitev) uporabnika, s čimer potrdi, da je ta upravičen do uporabe elektronske banke. Kot varen način prijave v elektronsko banko, ki ga banka omogoča se uporablja prijavno sredstvo Rekono. V okviru storitve Rekono se z uporabo močnih kriptografskih algoritmov in strojnih varnostnih modulov (ang. Hardware Security Module) zagotavlja varnost podatkov, kot so uporabniška gesla in enkratne kode. Vsi varnostno občutljivi podatki so tako varovani s kriptografskimi algoritmi, kot so zgoščevalne funkcije (SHA-256 ali močnejši), HMAC (zgoščevalna funkcija overjena s simetričnim ključem dolžine 256 bitov) in šifriranje z uporabo simetričnih ključev AES 256. Vse operacije s kriptografskimi ključi se izvajajo v strojnih varnostnih modulih.

Prijava uporabnikov elektronske banke s prijavnim sredstvom Rekono poteka po načelu močne avtentikacije, kjer sta od uporabnika zahtevana vsaj dva faktorja (od treh faktorjev: nekaj kar znaš, nekaj kar imaš, nekaj kar si), s katerima ta potrdi, da je upravičen do želenega dostopa. Faktorja sta med seboj neodvisna kar bistveno otežuje možnost zlorabe in pridobitev neupravičenega dostopa.

1.5 Varnostni sistem proti ugibanju gesla

V primeru, da ste petkrat zapored vnesli napačno kodo, ki vam je bila posredovana preko SMS, vam bo vstop v elektronsko banko popolnoma onemogočen. Za ponovno vzpostavitev pogojev za dostop in uporabo elektronske banke se boste morali osebno oglasiti v enoti banke.

V primeru napačne prijave ali v primeru, če se IP naslov v sklopu aktivne seje spremeni boste uporabniki, ki ste si funkcionalnost predhodno vklopili, prejeli SMS-obvestilo.

Omenjeni varnostni mehanizem onemogoča, da bi nepooblaščena oseba poskušala vstopiti v sistem z ugibanjem vašega gesla, vam pa omogoča pravočasno zaznavo morebitne nepooblaščene aktivnosti na vašem računu za takojšnje ukrepanje.

V primeru zaznave nepooblaščene aktivnosti na vašem računu nemudoma kontaktirajte banko.

1.6 Varnostni sistem samodejne odjave

Ko ste v elektronsko banko že prijavljeni in v času petih minut ne opravite nobenega ukaza ali klika z miško, vas sistem samodejno odjavi. Za nadaljevanje dela oz. za ponovni vstop v elektronsko banko se je potrebno ponovno prijaviti v sistem. **Po končanem delu se iz sistema**

elektronske banke vedno odjavite s klikom na izbirno vrstico "Odjava" in zaprite vsa okna brskalnika.

Prav tako se lahko z namenom dodatne varnosti, z enim uporabniškim imenom naenkrat prijavi samo en uporabnik. Sistem ne omogoča prijave istega uporabnika z več računalnikov hkrati.

Vsi parametri, ki se prenašajo v spletnem naslovu (URL naslovu), so šifrirani in jih ni mogoče uporabiti za dostop do podatkov na podlagi prepisovanja v drug računalnik.

Svetujemo vam, da po končanem delu elektronsko banko vedno zapustite s klikom na izbirno vrstico »Odjava«. V nasprotnem primeru namreč nekateri brskalniki omogočajo, da s klikom na gumb »Nazaj« (ang. Back) ponovno pridobite dostop do zadnje ogledanih spletnih strani.

1.7 Varnostni sistem ugotavljanja in dodatnega potrjevanja neobičajnih transakcij

Za dodatni nivo varnosti smo v elektronsko banko vgradili varnostni sistem neobičajnih transakcij. Sistem razpozna neobičajno transakcijo in od uporabnika zahteva podpis transakcije z vnosom enkratnega gesla, ki se izračuna na podlagi podatkov o prejemniku plačila in zneska plačila. Plačnik enkratno geslo prejme preko SMS sporočila. Funkcionalnost preprečuje tudi morebitno kasnejše nepooblaščeno spreminjanj plačilnih podatkov kjerkoli v postopku vnosa plačilnega naloga. Generirano enkratno geslo namreč temelji na tehnologiji dinamičnega povezovanja (ang. Dynamic Linking), ki onemogoča realizacijo plačila, če se plačilni podatki in vneseno enkratno geslo ne ujemajo.

Gre za dodatno varnostno funkcijo, ki preprečuje morebitne transakcije na transakcijske račune, ki niso navedeni v imeniku varnih plačil. To predstavlja dodatni varnostni mehanizem v primeru, da se nepooblaščena oseba seznani z vašimi prijavnimi elementi in si s tem zagotovi vstop v elektronsko banko. Prav tako ta funkcija preprečuje morebitno spreminjanj plačilnih podatkov v fazi izmenjave sporočil med spletnim brskalnikom in elektronsko banko, saj zazna, da se plačilni podatki in vneseno enkratno geslo ne ujemajo, glede na podatke na podlagi katerih je bilo to ustvarjeno.

2 Računalniška oprema za uporabo elektronske banke

2.1 Priporočljiva strojna oprema

- 1gHz ali hitrejši procesor,
- 2GB rama ali več,
- 16GB trdega diska.

2.2 Operacijski sistem

Elektronska banka deluje na vseh operacijskih sistemih, ki podpirajo šifriranje spletnih strani. **Za varno in optimalno delovanje elektronske banke priporočamo uporabo operacijskega sistema Microsoft Windows 10 ali novejšega.**

2.3 Internet povezava

Dostop do interneta z možnostjo uporabe spletnih brskalnikov oz. pregledovalnikov Internet Explorer, Mozilla Firefox, Google Chrome itd.. Priporočamo uporabo dostopa do interneta prek zanesljivih slovenskih ponudnikov, ki nudijo kvalitetne in hitre povezave.

- ***Požarna pregrada***

Uporabniki DBS NET-a, ki dostopajo v internet iz omrežij prek požarne pregrade, morajo zagotoviti, da sta na njem odprta naslednja porta (vrata), ki morata biti odprta v obe smeri:

  - PORT 80 (HTTP) in
  - PORT 443 (SSL).

- ***Spletni brskalnik***

Priporočamo uporabo najnovejših brskalnikov ali vsaj Internet Explorer 11.

Potrebna je uporaba spletnih brskalnikov, ki podpirajo 256-bitno TLS (ang. Transport Layer Security) šifriranje in omogočajo visoko varnost pri uporabi elektronske banke. Vsi novejši brskalniki omogočajo tovrstno šifriranje.

2.4 Posodobitve operacijskega sistema in spletnih brskalnikov

Za varno in nemoteno uporabo elektronske banke je nujno, da si na osebnih računalnikih, na katerih dostopate do elektronske banke, redno nameščate vse najnovejše varnostne popravke in posodobitve, ki jih izdaja izdajatelj operacijskega sistema in ostali proizvajalci programske opreme, ki jo imate nameščeno na vaši napravi. Posebno bodite pozorni tudi na redno posodabljanje spletnega brskalnika.

3 Splošna varnostna priporočila za uporabnike elektronskega bančništva

Banka uporabnikom elektronskega bančništva svetuje, da za izboljšanje varnostne zaščite upoštevajo spodnja priporočila:

- Dostop do osebnega računalnika oz. naprave, ki jo uporabljate za dostop do elektronskega bančništva zaupajte samo osebam, ki jim zaupate.
- Pozorni bodite na elektronska sporočila, ki vas napeljujejo na lažne spletne strani. Nikoli ne klikajte na povezave, ki vam jih pošilja neznan pošiljatelj.
- Ne odpirajte priponk, ki vam jih pošilja neznan pošiljatelj.
- Ko zaključite z delom v elektronski banki, se odjavite. Nikoli se ne oddaljujte od računalnika medtem ko imate odprt elektronski bančni račun.
- Za dostop do elektronske banke uporabljate izključno naprave, ki niso javno dostopne.
- Na osebni računalnik oz. napravo, ki jo uporabljate za dostop do elektronske banke, ne nameščajte programske opreme iz nepreverjenih virov in nelegalno pridobljene programske opreme.
- Na osebnem računalniku uporabljate požarno pregrado, ki je del nameščenega operacijskega sistema.
- Če med delovanjem elektronske banke opazite neobičajne ekrane ali izrazito počasnejše delovanje je to lahko znak, da je na vašem računalniku nameščena zlonamerna programska oprema. Svetujemo vam takojšnjo prekinitev uporabe elektronske banke in izključitev naprave iz internetnega omrežja, dokler strokovno usposobljena oseba (informatik) ne opravi pregleda naprave.
- Ne uporabljajte elektronske banke, če imate hkrati odprta tudi druga spletna mesta oz. zavihke v spletnem brskalniku.
- Nikomur ne zaupajte vaših gesel, ki jih uporabljate za dostop do elektronske banke. Ta gesla poznate samo vi zato je pomembno, da ostanejo tajna. Pri oblikovanju gesel upoštevajte, da so ta dolga vsaj 8 znakov in kompleksna (kombinacija majhnih in velikih črk, številk ter posebnih znakov). Za različne sisteme/programe uporabljajte različna gesla. Gesel ne shranjujte v brskalnik.
- Banka od vas nikoli ne bo zahtevala razkritje vašega gesla.
- Na napravi, s katero dostopate do elektronske banke, priporočamo, da uporabljate posodobljeno protivirusno zaščito (anti-virusni program). Ta vas lahko uspešno varuje pred virusi, trojanskimi konji, črvi in drugo zlonamerno programsko opremo.
- Za dostop do elektronske banke vselej uporabite internetno povezavo za katero ste prepričani, da nanjo niso priključeni neznani uporabniki. Interneta povezava, ki jo uporabite za dostop do elektronske banke naj bo vselej zaščitena z geslom. Ne uporabljajte javnih internetnih povezav v nakupovalnih centrih, letališčih, gostilnah ipd.
- Ažurne informacije o pogostih varnostnih grožnja, ki se pojavljajo pri uporabi elektronskega bančništva in spletnih plačil, lahko najdete na javni spletni strani Deželne banke Slovenije d.d., in sicer preko podstrani E-varnost.
- Več uporabnih varnostnih napotkov lahko vselej najdete tudi na spletni strani Varni na internetu.