INTERNETIPANGA TEHNILISED TINGIMUSED

Tehnilised nõuded LHV Internetipanga kasutamiseks

LHV Internetipanga võimaluste täielikuks kasutamiseks peab kasutaja tuvastama end ID-kaardi, Mobiil-ID või PIN-kalkulaatori abil.

ID-kaardiga töötavad hästi:

- Microsoft **Windows** operatsioonisüsteemidel (alates versioonist XP) brauserid Microsoft **Internet Explorer** (alates versioonist 7) ja **Mozilla Firefox** (alates versioonist 3).

  Muude brauseritega võib, aga ei pruugi õnnestuda sisselogimine ja/või maksete allkirjastamine.
- Apple **Macintosh** operatsioonisüsteemidel (alates versioonist 10.6.x) vaid **Firefox** (alates versioonist 3).
  Safariga ID-kaardi abil LHV Internetipanka sisenemine tõenäoliselt ei õnnestu.
- **Linux** operatsioonisüsteemidel **Firefox** (alates versioonist 3).

  Lynxiga ID-kaardi abil LHV Internetipanka sisse logida ei õnnestu.

Mobiil-ID ja **PIN-kalkulaatori** abil kasutaja tuvastamiseks ja maksete allkirjastamiseks peab kasutatavas brauseris töötama lisaks **JavaScript**.

Turvalisus LHV Internetipangas

LHV Internetipanga arendamisel on turvalisus esmase tähtsusega tegur. Oluline roll on samas ka Internetipanga kasutajal endal ja tema kasutataval riist- ja tarkvaral. Internetipanga kasutamine on nii turvaline kui turvaline on nõrgim lüli kogu süsteemis.

1. Pank teeb internetipanga turvalisuse tagamiseks järgmist:

- Internetipanga kasutaja ja panga vaheline informatsioon krüpteeritakse (SSL3 või TLS1 meetodi abil HTTPS protokollil).
- Internetipanga kasutaja tuvastatakse unikaalse tunnuse ning ID-kaardi, mobiil-ID või PIN kalkulaatori abil.
- Kui kasutaja üritab tulutult sisse logida rohkem kui 5 korda, siis PIN kalkulaator lukustub.
- Internetipanga sessioon aegub.

2. Klient/kasutaja peab omalt poolt tegema järgnevat:

- LHV Internetipanga avanedes veenduma, et brauseri aadressireal oleks õige aadress (https://www.lhv.ee) ning et ühendus oleks krüpteeritud.
  Autentsust ja krüpteeritust tunnistab brauseri aadressireal roheliselt kuvatav sertifitseeritu nimi (AS LHV Pank [Ee]), sertifitseerija nimi (Thawte) ja suletud tabalukk (mis võib olla ka brauseri akna alumisel serval).
- Hoidma oma kasutajatunnust ja identifitseerimisvahendeid turvaliselt.
  LHV Internetipanga kasutaja identifitseerimine kasutajatunnuse ja PIN koodide sisestamise abil toimub vaid Internetipanga elektroonilises keskkonnas. LHV Panga esindajad ei küsi Sinu paroole ega PIN koode mitte kunagi. Kui keegi pärib Sinult kasutajatunnust või PIN koode telefonitsi, e-posti teel või muul moel, keeldu ja teata toimunust kohe LHV klienditoele.
  ID-kaardi kaotamisest tuleb koheselt teavitada ID-kaardi abiliini 1777, mobiil-ID kaotamisest SIM kaardi väljastanud teenusepakkujat ning PIN kalkulaatori kaotamisest LHV kliendituge.
- Määrama mõistlikud ja oma vajadusi mitte ületavad limiidid ühe päeva ja kuu jooksul teha lubatud tehingute summale.
- Kaitsma Internetipanka logimiseks kasutatavat arvutit ja selle tarkvara (vt ka „Internetist ja turvalisusest üldiselt“).
- Internetipanga kasutamise lõpetamisel logima internetipangast välja – nupp LOGI VÄLJA internetipanga lehe päises.

3. Turvaelemendid

LHV Internetipanga kasutaja identifitseerimine toimub turvaelementide abil. Panga väljastatavad turvaelemendid on Panga poolt kehtestatud korras kasutajale antav unikaalne kasutajanimi ja PIN-kalkulaator, mille abil saab kasutaja siseneda Internetipanka. Lisaks PIN-kalkulaatorile saab kasutaja tuvastada end ka Mobiil-ID või ID-kaardi abil.

Soovi korral saab endale määrata ajutise kauplemisparooli ja ajutise parooli LHV foorumite kasutamiseks. Paroolide kasutamist LHV ei soovita. Kui siiski on soov ajutisi paroole kasutada, peab salasõna olema võimalikult pikk, sisaldama võimalikult palju erinevaid märke ega tohiks sisaldada isiklikku informatsiooni,

mida oleks lihtne ära arvata. Samas peaks salasõna olema piisavalt hästi meeldejääv, et ei oleks vaja seda üles kirjutada.

Kui Sul on kahtlusi, et Sinu kontot kasutab keegi teine või leiad, et LHV Internetipanga turvalisusega on probleeme, helista palun kohe meie klienditoele (+372 6 800 400).

Internetist ja turvalisusest üldiselt

Internet kui oht

Internet oli kord suletud võrk, mis ühendas usaldusväärseid arvuteid ja haritud kasutajaid. Selle infrastruktuuri toimimise loogilised alused kirjeldati 70'ndatel aastatel lähtudes usaldusest ja lihtsusest ning turvalisusele pöörati vähe tähelepanu.

Täna tegutsevad selles samas, kuid üleilmseks kasvanud keskkonnas muuhulgas küberkurjategijad, kelle edukus sõltub arvutite, kaasa arvatud Sinu arvuti ärakasutamise efektiivsusest ja varastatava informatsiooni tõhusast pruukimisest (muuhulgas Sinu krediitkaartide andmed, internetipanga paroolid jms). Küberkurjategijate tegutsemise teeb hõlpsaks tõik, et interneti infrastruktuuri loogilised alused on täna sisuliselt sama ebaturvalised kui paarkümmend aastat tagasi, kui võrgus olid vaid usaldusväärsed liikmed ning kõik usaldasid kõiki.

Seepärast on Sinul, internetikasutajal mõistlik võimalike kahjude vältimiseks järgida põhimõtteid, millest põhjalikult kuid lihtsas keeles on kirjutatud lehel arvutikaitse.ee.

Sinu harjumustest sõltumatud ründed

Internetti või kohtvõrku ühendatud arvuti võib olla üsna kaitsetu – ka värskelt installeeritud MS Windows operatsioonisüsteem „kuulab" võrgust lähtuvaid teateid ning vajadusel vastab neile. Selline teenus on näiteks „*File and Printer Sharing*".

Eesmärgipäraselt koostatud päringuga võib oskuslik kurjategija raali valvsust aga petta (nn *remote exploit*) ning saavutada ligipääsu arvuti omaniku dokumentidele, paigaldada pahavara või arvuti sootuks sandistada.

Kuidas end kaitsta?

Reeglina aitab selliste rünnete vastu õigesti seadistatud tulemüür (*firewall*) ja toimiv viirustõrje. Viiruseid tõrjuva tarkvara pakkujaid on palju, kuid MS Windowsi kasutajatel soovitame valida näiteks nende hulgast.

Lisaks peab kindlasti paigaldama nii operatsioonisüsteemi, viirustõrje kui ka arvutis kasutatava tarkvara uuendusi.

Microsofti operatsioonisüsteemid pakuvad tarkvarauuendusi automaatselt (kui kasutaja seda just eraldi keelanud pole). Käsitsi saab neid paigaldada siit.

Arvutis kasutatava tarkvara täiendused saab laadida tarkvaratootja kodulehelt või uuendatava programmi abil.
Näiteks Adobe Readeri puhul *help* menüüs valik *check updates*.

Kindlasti peab värskena hoidma Adobe Flash'i, sest selle vigu kasutatakse veebipõhiste rünnete puhul väga sageli. Olemasolevat versiooni saad kontrollida siin ning värskeima laadida siit.

Kui kasutad näiteks LHV Traderit, on Sinu arvutis kindlasti ka Java. Selle täiendusi pakub Java programm ise ning neid peab kindlasti paigaldama.

Mac OS X värskendamiseks peab aegajalt õuna pildiga menüüst valima „Software Update..." ning laskma arvutil vajalikud täiendused paigaldada.

Linuxi operatsioonisüsteemide puhul sõltub uuenduste paigaldamise metoodika kasutatavast distributsioonist. Reeglina peab root kasutaja õigustes käsurealt käivitama vastavad käsud. Näiteks:

- Ubuntu (ühel real 4 käsku, kõik vajalikud)
  aptitude update && aptitude safe-upgrade && aptitude dist-upgrade && aptitude safe-upgrade
- RedHat
  yum update
- Mandriva
  urpmi-update -a

Sinu harjumusi ära kasutavad ründed

Ohtlikumad ja levinuimad on tänapäeval kasutaja (teadmatul) kaasabil toimuvad ründed (nn *client side attack*). Näiteks saadetakse Sulle e-mail, millele on manusena lisatud .pdf, .doc, .jpg, .xlsx või muu laiendiga fail, mille avamisega oled harjunud ning mille avamiseks vajalik tarkvara on Sul olemas.

Et saadud kirja sisu tundub usutav (näiteks kutsutakse seminarile ning kava olevat .pdf dokumendis), avad manusena lisatud faili Adobe Acrobat Reader'i abil, tutvud sisuga, sulged faili ja unustad selle mõne minuti pärast.

Kuid dokumendi avamisel käivitas programm selles sisaldunud salakavala koodi, mis paigaldas Sinu masinasse klahvivajutuste salvestaja ja peidetud tagaukse, mille kaudu ründe autor Sinu arvuti üle võimust võtab. Sinu viirustõrje selles probleemi ei näe, sest ründeks kasutatud meetodit programm veel kurjaks pidada ei oska – see teave jõuab tõrjeprogrammini alles mõne tunni või halvemal juhul mõne kuu pärast.

Kurja koodi sisaldavad failid ei pruugi tulla vaid e-postiga. Levinud on ka MSN, Facebook jt palju kasutatavate suhtluskanalite kaudu toimuvad ründed, kus Sinu sõber (justkui) saadab sulle faili, mida soovitab avada või aadressi, millele brauseriga minna. Faili avamisel toimub sama, mida eespool kirjeldatud, veebiaadressi avamisel kasutatakse ründamiseks aga Sinu brauseri turvaauku.

Hästi sooritatud ründest ei saa kasutaja, ehk Sina reeglina teada enne, kui krediitkaardilt või pangakontolt raha kaduma hakkab.

Kuidas end kaitsta?

- Enne e-postiga tulnud faili avamist mõtle, kas selle saatja on usaldusväärne ning kas ta on varem selle faili saatmisest Sulle teatanud.
- Kui surfad internetis mõtle, kas lehekülg, millele sul soovitatakse minna, on usaldusväärne.
- Kui leiad pealtnäha vahva programmi, *screensaver*'i või oma brauserile uue *toolbar*'i mõtle, kas Sul seda ka tegelikult vaja on ning kas see kaalub üles võimaluse kaotada pangakontol olev raha.
- Kui kodus on mitu arvutit, kasuta neist vaid ühte Internetipangas käimiseks, krediitkaardimaksete tegemiseks jm oluliseks. Selle arvuti puhul jälgi eriti hoolikalt, mida Sa sellega teed – millistel veebilehtedel käid, milliseid faile avad, millist tarkvara sinna paigaldad.

Sinu ID-Kaart, Mobiil-ID ja PIN kalkulaator

ID-kaart on suhteliselt turvaline seepärast, et kui ründaja ka jälgib iga Su klahvivajutust (ja saab teada nii Sinu PIN1 kui PIN2 koodi), ei saa ta siiski Sinu pangakontole ligi, sest autoriseerimiseks on vaja füüsilist eset – Sinu ID-Kaarti. Seda tal aga elektroonilisi kanaleid pidi varastada ei õnnestu.

Sama kehtib Mobiil-ID ja PIN kalkulaatori kohta, kuid erinevalt ID-kaardist ei pea PIN kalkulaatorit või mobiil-ID-d arvutiga ühendama.