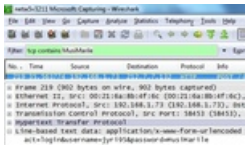
Kuidas hoiduda paroolide internetis lekkimisest?

27. oktoober 2010 - 22:00 Autor: AM

(Arvutimaailm 3/10)



? Kuidas vältida seda, et pärast veebilehel parooli sisestamist ei lekiks kasutajate krüpteerimata salasõnad? Et pätid ei teeks nende Paypali kontot tühjaks või ei kirjutataks rõvedusi veebiprofiilidesse?

! Veebilehe liikluse, sealhulgas paroolide salastamiseks on vaja kahte asja: eraldi IP-aadressi ning turvasertifikaati.

Veebipidajad peavad hoolitsema oma klientide paroolide turvalisuse eest igal tasandil. Kuid ka kasutajad peavad teadvustama, et kasutades erinevates kohtades sama parooli tekitab ühe veebipidaja hoolimatus talle teises kohas rahakotile või mainele otsest käegakatsutavat kahju.

Enamik internetikasutajaid ei oska arvatagi, et pärast parooli sisestamist ükskõik kas mõnes suuremas või väiksemas veebis muutub see nähtavaks peaaegu igaühele, kes viitsib selle vaatamiseks vaeva näha. Samas on lihtsate vahenditega võimalik korraldada nii, et isegi veebilehe omanikul ei ole võimalik su parooli teada saada, kasutades näiteks OpenID-taolist kasutajate autentimist turvalises kohas.

Salapärane https://

Võrguliiklust, sealhulgas paroole on juhtmeta võrgu ajastul raske kõrvalvaatajate eest peita. Lihtsustatult öeldes on paroolid avalikud, kui sisened näiteks rate.ee lehele kooli WiFi-võrgus, kuhu võib samal ajal olla ühendatud ka keegi teine. Kuid lihtne on ka muuta andmed selliseks, et kõrvalised isikud sellest aru ei saa – seda kutsutakse krüpteerimiseks. Veebis on standardiks https protokoll. Kui aadressiriba alguses on „https://", siis serverisse minevad ja tulevad andmed on krüpteeritud.

Veebilehe krüpteeritavaks muutmiseks on vaja vaid kahte asja – eraldi IP-aadressi ning sertifikaati. Sertifikaatide hinnavahemik on 10–2000 USA dollarit aastas. Ühed odavamad sertifikaadid on müügil näiteks namecheap.com lehel. Need sobivad veebilehe krüpteerimiseks 99% juhtudel. Kallimate eelised on kuulus brand, kindlustus ning mõnevõrra suurem vanade ja vähekasutatavate brauserite tugi. Namecheapi veebimajutuse hinnakirja järgi on eraldi IP-aadressi hind 30 USA dollarit aastas. Kokku on elementaarse turvalisuse hind veebilehele seega *ca* 40 krooni kuus.

Kasuta eri paroole

Kindlasti ei tohi rate.ee parool olla sama, mis Paypalil või internetipangas. Sellistel tähtsatel teenustel, kus parooli leke tähendab otsest rahalist kadu, peab olema igal oma unikaalne salasõna. Kõikvõimalike erinevate veebilehtede jaoks aga ei jõua keegi meeles pidada kümneid unikaalseid paroole. Lehtedel, kus paroole hoitakse korralikult ja mis ei põhjusta olulist kahju, kui konto pättidele kättesaadavaks saab, võib tavakasutaja kompromissina kasutada korduvat parooli.

Lahendus harva kasutatavate veebikohtade juures on ühekordsed paroolid: valid mõne suvalise salasõna ning järgmine kord kasutad parooli meeldetuletust. Samas leidub palju selliseid lehti, kus kedagi ei huvitagi, kas parool on avalik või mitte, nende lehtede jaoks võib olla meeles üks ühine lihtne parool.

Kasutada võib ka paroolide haldusprogramme, ühe sellise saab aadressilt moonsoftware.com/pwagent.asp. Kuid on veel abilisi, mis paroolidega majandada aitavad. Wireshark näiteks kontrollib, kas lehel sisestatud parool on avalik või mitte. Iga võrguliikluse sõnumi kohta näitab Wireshark selle sõnumi sisu, kui seal on näha oma parool, siis näevad seda ka kõik teised. Enne salasõna sisestamist tuleb Wireshark käima panna ning kasutada filtrit „tcp contains salasõna", asendades salasõna oma parooliga. Kui nüüd mõni sõnum leitakse, siis on selge, et paroolid sellel veebilehel võetakse vastu avalikena.

Mida vastati ebaturvalise parooliga lehekülgedelt?

Küsisin paari populaarsema veebilehe käest, miks neil turvalist https-ühendust ei kasutata ja miks paroolid saadetakse serverisse krüpteerimata. Vastused on sellised.

Rate.ee. Saatsin „Idee või ettepanek" sektsioonis klienditoele teate. Vastuseks sain: „Tere,? Tervitades, Rate.ee meeskond."

Arvatavasti ei saadud minust aru ning sõnastasin küsimuse ümber. Kolm päeva on loo kirjutamise ajal möödas ja vastust pole tulnud.

cvkeskus.ee. Vastus: „CV Keskus kasutab tehnikat, mida enamik portaale. See ei ole ebaturvalisem kui mõnel teisel samalaadsel lehel." Küsiti, kuidas probleemi lahendada. Pärast lahenduse selgitamist tänati ettepaneku eest ja lubati edastada see arendusosakonnale.

ilm.ee. Lihtne ja lühike seisukoht: „Lihtsuse huvides kasutab enamik keskkondi, kus kasutajanime taga pole ei raha ega muud olulist, sama lähenemist."

auto24.ee. Asjast oldi teadlikud: „Antud muudatus on meil plaanis."

Positiivsed näited

Positiivse lõpu huvides võrdluseks ka paar probleemivaba näidet:

- osta.ee
- forumcinemas.ee
- koosakyla.ee
- ee.ekool.eu
- markit.eu

MARGUS PALA
IT-spetsialist

Pildil: Wiresharki ekraanipildilt on näha, kuidas turvamata parool filtrisse jääb.

- Lahendused
- Turvalisus