



Kahe-faktoriline autentimine kaitseb identiteedi varguste eest

Autor: Hardy Viilup

Tavaliselt põhineb autentimine korduvkasutatavatel staatilistel paroolidel. Pikad ja keerukad paroolid on turvalisemad aga samas on neid raske meelde jätta, selle tõttu kirjutatakse paroolid üles või kasutatakse lühikesi, nõrku paroole. See võimaldab ründajatel tuvastada kasutaja parooli ja varastada tema identiteedi.

Paljud ründajad ei vaevu enam kasutajate paroole “muukima”, selle asemel püütakse nakatada rünnatava isiku arvuti klahvivajutuste registreerijaga, mis edastab tuvastatud kasutajatunnused ja paroolid ründajale, kes võib seeläbi omastada rünnatava isiku identiteedi.

Kahe-faktoriline autentimine kaitseb edukalt identiteedi varguste eest. Kahe-faktoriline autentimine tähendab, et sulle on teada mingi saladus, näiteks PIN ja sul on midagi, näiteks PIN kalkulaator. Selline lahendus välistab kasutajatel lühikeste paroolide kasutamise, samuti pole neil vajadust meeles pidada pikki, keerukaid paroole.

Et tagada kõrgem turvalisus, kasutatakse PIN kalkulaatorites ajast sõltuvaid paroolivahetusalgoritme. Parool vahetub tavaliselt minutilise intervalliga, seega iga parool on kasutatav vaid minut aega. Et välistada ründajate poolt paroolide nn. “korduv-kasutust”, kasutatakse lahenduses parooli lukustamist, st. juba kasutatud parooli ei saa teist korda kasutada.

Pikka aega on sellised autentimislahendused kasutusel olnud veebiserveritesse, WiFi võrkudesse, e-posti ja VPN serveritesse autentimiseks. Nüüd on võimalik kasutada lahendust ka MS Windows domeenidesse autentimise turbeks. Toetatud on ka autonoomne režiim, st. kasutajal on võimalik lokaalsesse masinasse sisse logida ka siis, kui domeen ei ole kättesaadav.

Tuntuimad tootajd:

RSA – <http://www.rsa.com>

Vasco – <http://www.vasco.com>

PassGo – <http://www.passgo.com>