Ekspert selgitab: isikutuvastamisel vaid kasutajatunnuse ja salasõna kasutamine on liiga ohtlik

10 kuud tagasi - 14.06.2025 Autor: AM

Selleks, et kaitsta end identiteedivarguse eest, tuleb nii isiklikes kui ka tööalastes tegemistes hakata kasutama isikutuvastamisel meetodeid, mis ei seo inimest ühe kindla salasõnaga.

Eri rakenduste ja teenuste kasutamisel on jätkuvalt kõige levinum autentimisviis kombinatsioon kasutajatunnusest ja salasõnast. Sellele on mõnel juhul lisandunud biomeetrilised tuvastusviisid, mida sageli kasutatakse ka hoopis alternatiivina kasutajatunnuse ja parooli sisestamisele.

"Üha populaarsemaks on muutumas ka ühekordsed paroolid ehk OTP-d, mida kasutatakse täiendava turvakihina," selgitab Telia küberturbe lahenduste arhitekt Kristjan Aljas, "need paroolid genereeritakse spetsiaalses mobiilirakenduses või teenusepakkuja pilveteenuses ning edastatakse kasutajale näiteks e-posti või SMS-i teel."

Kuigi selline lisakaitse sisselogimisel võib tunduda piisav, tõdeb Aljas, et tegelikult on küberkurjategijad juba leidnud viise läbi eri õngitsusskeemide ja vahendajarünnete, kuidas ikkagi märkamatult soovitud andmetele ligi pääseda.

"Sellise riski maandamise üks võimalus oleks digitaalsete tuvastusvahendite täiendamine mõne füüsilise komponendi või seadmega, millele ligipääsu omamata ei ole autentimist lõpuni viia võimalik. Hea näide on Eesti ID-kaart, mille põhiprobleem on aga piiratud kasutusvõimalus, kuna globaalsetel platvormidel ja teenustel pole sellega liidestatust," lisab ta.

Füüsiline turvavõti hakkab salasõnu asendama

Kuna autentimisstandardeid arendav ühendus FIDO Alliance on võtnud suuna salasõna-põhisest isikutuvastusest järk-järgult loobumisele, tuleks ka Eestis teha samme selles suunas. Üks võimalus on asjatundja sõnul maailma juhtiva turvavõtmete tootja Yubico pakutav turvavõti YubiKey. Seda kasutavad juba USA ja Euroopa paljud valitsusasutused ning rahvusvahelised finantsorganisatsioonid,

kes on nüüdseks säästnud juba sadu miljoneid eurosid, mis muidu oleks kulunud pettuste ja küberrünnakutega tehtud kahju likvideerimiseks.

"2025. aasta uuringute kohaselt on IT- ja OT-süsteemide kaitsmiseks mõeldud paroolivaba autentimine võetud laialdaselt kasutusele juba tervishoius, energeetikas ja valitsusasutustes," räägib Aljas. Lisaks salasõnadest ja nendega seotud probleemidest vabanemisele on YubiKeyl tema sõnul eeliseid veel. Näiteks võimaldab turvavõti isikutuvastust pilveteenuste platvormidel ning see ühildub paroolihaldurite ja kesksete identiteedi- ning autentimisplatvormidega. Kuna YubiKey võtmed on saadaval eri korpustes ja nii USB-, NFC- kui ka Lightning-liidestega, on neid lihtne kaasas kanda ja need toimivad enamikus seadmetes.

Toetamaks FIDO Alliance-i salasõnadest loobumise põhimõtet, kuuluvad Aljase sõnul YubiKey-del põhinevad isikutavastuslahendused ka Telia küberteenuste portfelli. Kuna füüsilise turvavõtme laiem kasutuselevõtt tähendab ka seda, et turule tuleb seadmeid, mille turvalisuses ei saa olla kindel, soovitab ta enne nende kasutuselevõttu arutada mõne spetsialistiga.

"Kindlasti tuleks kriitiliste turvalahenduste ning seadmete ostmisel kasutada tootja ametlikku müügikanalit ja volitatud partnereid," rõhutab Aljas, "vältima peab soodsamana näivaid veebipoode ja tarnekanaleid, kus puudub võimalus tuvastada, kellel ja millisel eesmärgil on olnud ligipääs ostetud seadmetele ja kas nendega on transpordi või ladustamise käigus manipuleeritud."

YubiKey juurutamisel on hea võtta appi mõni kogenud partner, kes aitab teha vajalikud seadistused, leppida kokku protseduurid ja koolitada töötajad.

- Lahendused

- Tarkvara
- Turvalisus

Pilt


delete
return
shift