EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE
it akadémia

Modul 12: Bezpečnosť pri využívaní IKT

Riadenie prístupu

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
www.itakademia.sk
ITMS2014+: 312011F057

4 Riadenie prístupu

4.1 Metodika

4.1.1 Opatrenia na zamedzenie neautorizovaného prístupu k údajom (používateľské heslo, PIN, šifrova-nie, viacfaktorová autentifikácia)

Heslo je všeobecný prostriedok slúžiaci na overenie totožnosti používateľa. Používateľ je považovaný za oprávneného, ak preukáže znalosť hesla.

PIN (z anglického personal identification number - osobné identifikačné číslo) - identifikátor, pomocou ktorého je možné sa autorizovať napr. pri platobnej karte, mobilného telefónu a pod. Najčastejšie sa jedná o štvormiestne číslo, ktoré sa musí zadať pri zapnutí (použití) predmetu a bez jeho znalosti nie je možné tento predmet použiť.

Šifrovanie dát je proces, ktorým sa nezabezpečené dáta prevedú pomocou kryptografie na dáta šifrované (čitateľná iba pre majiteľa dešifrovacieho kľúča).

Viacfaktorová autentifikácia je metóda riadenia prístupu, pri ktorej bude používateľovi udelený prístup na základe úspešného prekonania niekoľkých oddelených bezpečnostných prvkov autentifikačného mechanizmu – typicky minimálne 2 z nasledovných: vedomosť (niečo, čo používateľ vie, napr. heslo alebo PIN), vlastníctvo (niečo čo používateľ má, napr. mobilný telefón s daným číslom alebo platobnú kartu) a fyzický znak (niečo, čo má používateľ vrodené a unikátne (biometrické údaje), napr. odtlačok prsta, sken dúhovky oka).

4.1.2 Jednorazové heslo (one-time password) a jeho využitie

Jednorazové heslá sa používajú väčšinou ako jeden z prvkov viacfaktorovej autentifikácie, prípadne ako prvotné heslo pre prihlásenie do počítačového systému, ktoré je nutné zmeniť po prvom úspešnom prihlásení. Pri viacfaktorovej autentifikácií je to typicky heslo, ktoré potvrdzuje napríklad vlastníctvo mobilného telefónu s istým telefónnym číslom. Takéto heslo má obmedzenú platnosť - dá sa použiť iba raz, čiže v prípade, že by ho útočník odchytil, nie je možné ho použiť znova. Často majú tieto hesla aj obmedzenú časovú platnosť (rádovo niekoľko minút). Napr. v bankovníctve sa využíva zasielanie jednorázového kľúča (PIN) cez SMS pri potvrdzovaní prevodu peňazí.

4.1.3 Účel sieťového účtu

Hlavným účelom sieťového účtu na rôznych sieťových službách je regulovať prístup jednotlivých používateľov k sieti, údajom počítačového systému. Na autentifikáciu k sieti sa používa meno a heslo, prípadne certifikát. Ak nedôjde k úspešnej autentifikácii používateľa, prístup do siete je mu odoprený.

4.1.4 Prístup k používateľskému účtu cez používateľské meno a heslo, nutnosť odhlásenia pri nepoužívaní

K účtu sa pristupuje pomocou mena a hesla. Meno definuje o ktorý účet sa jedná a znalosť hesla autorizuje používateľa k práci s účtom. Ak dotyčný prestane pracovať

s účtom, je dôležité sa odhlásiť z tohto účtu. V prípade kratších prestávok v práci je možné účet na počítači dočasne zablokovať, aby v prípade neprítomnosti nemohol byť účet zneužitý.

4.1.5 Bežné techniky riadenia prístupu k sieti na základe biometrických údajov (odtlačky prstov, obraz dúhovky oka, rozpoznávanie tváre, geometria dlane)

Každý ľudský organizmus je svojím spôsobom unikát a na ľudskom tele sa nachádza niekoľko unikátnych znakov (tzv. biometrických údajov), ktoré možno pomocou dnešnej technológie ľahko digitalizovať a použiť tak k overeniu totožnosti používateľa. Pri autentifikácii pomocou biometrických údajov sa získaná vzorka uloží a priradí k používateľovi a pri prihlasovaní sa načítaný údaj porovná s uloženým a na základe porovnania prihlási používateľa.

Najčastejšie sa využívajú **odtlačky prstov**. Ich snímače sú pomerne lacné a už niekoľko rokov sú súčasťou výbavy niektorých notebookov a nedávno sa dostali aj do mobilných telefónov. U jednoduchších býva chybovosť lepšia ako 1%, v prípade profesionálnych (bezpečnostné firmy a pod.) klesá pod 0,001%.

V súčasnosti sa pripravujú zariadenia pre **skenovanie dúhovky** oka pre nasadenie do mobilných zariadení, kde by mala byť chybovosť do 0,001%. Skenovacie zariadenia používané na niektorých letiskách majú chybovosť pod 0,000001%, čo predstavuje jednu chybu na 100.000.000 pasažierov.

Ďalšími možnosťami zabezpečenia pomocou biometrických údajov sú napríklad **rozpoznávanie tváre** (podľa geometrických charakteristík tváre) a **geometria dlane** (ruka je tiež do istej miery jedinečná - neposkytuje však dostatok informácií a preto sa odporúča používať výlučne v priestoroch s nízkym počtom pohybujúcich sa osôb).

4.2 Správa hesiel

4.2.1 Zásady pre výber hesiel (primeraná dĺžka, zložitosť, nezdieľanie hesla, pravidelná zmena hesla, rozdielne heslá pre rôzne služby)

Na zabezpečenie potrebnej úrovne ochrany používateľských účtov pri prihlasovaní menom a heslom je dôležité stanoviť pravidlá pre tvorbu hesiel.

Základnými parametrami sú dĺžka hesla a povinná kombinácia znakov (veľkých a malých písmen, číslic, prípadne špeciálnych znakov). Takto dosiahneme, že používateľove heslá sú dostatočné pre odolávanie tzv. útoku hrubou silou (útok, pri ktorom počítačový program skúša zaradom všetky možné kombinácie znakov), resp. tzv. slovníkovému útoku (program skúša zaradom všetky heslá z vopred zostaveného slovníku, napríklad bežných slov nejakého jazyka a podobne).

Snáď ani netreba pripomínať, že heslo je tajná informácia, a preto je obrovským rizikom zdieľať prístupové heslo s inými osobami. Na takéto účely slúžia viaceré používateľské účty k jednej službe.

Pri častom používaní hesla sa môže stať, že ho niekto nepovolaný zistí, preto je vhodné heslo po nejakom čase zmeniť. Môže to vykonať používateľ na základe vlastného rozhodnutia, alebo túto požiadavku môže mať jeho organizácia uvedenú v pracovnom poriadku resp. v pravidlách pre používanie siete, prípadne zmenu môže vyžadovať autentifikačný systém. Pre zvýšenie ochrany sa môžu špecifikovať doplnkové pravidlá pre zmenené heslá, typicky napr. nie je možné použiť niekoľko naposledy použitých hesiel, heslo sa musí od predchádzajúceho dostatočne odlišovať (ak mám heslo "Heslo1", nemôžem si nastaviť nové heslo "Heslo2").

Dôležitým aspektom dnešnej doby je nepoužívať rovnaké heslo pre viacero služieb. Môže sa totiž stať, že konkrétna služba neudržuje databázu hesiel dostatočne zabezpečenú a pri útoku na túto službu môže Vaše heslo uniknúť, pričom Vy sa toto väčšinou ani nedozviete. Vaše heslo (aj keď je zložité) je potom v rukách útočníka a spolu s ním aj prístup k ďalším službám.

4.2.2 Softvér na správu hesiel

V dnešnej digitálnej dobe sa denne stretávame s nutnosťou autorizovať sa heslom takmer všade. To so sebou prináša potrebu pamätať si množstvo hesiel, čo sa s pribúdajúcim počtom stáva neúnosným. Situáciu riešia tzv. manažéri hesiel, čo sú špecializované programy slúžiace na ukladanie hesiel - heslá sú uložené v zašifrovanej databáze, čiže relatívne bezpečne. Používateľ si nemusí pamätať všetky heslá, pamätá si iba jedno, ktoré slúži k zašifrovaniu a opätovnému dešifrovaniu databáze. Jednoduché varianty týchto manažérov obsahujú v dnešnej dobe aj webové prehliadače.