Tema: Controlul accesului în sistemele informatice

1. Metode de autentificare

Controalele sunt impuse pentru a diminua riscurile la care sunt expuse sisteme informaționale și pentru reducerea potențialelor pierderi. Controalele vizează responsabilizarea persoanelor care accesează informații sensibile.

Responsabilizarea este înfăptuită prin mecanisme de control al accesului care exercită funcțiile de *identificare, autentificare, autorizare și auditare.*

Autentificarea este procesul de stabilire că un obiect sau un subiect sunt adevarate, asa cum cineva pretinde - procesul de verificare a identitatii digitale.

Autorizarea este procesul prin care unei entități particulare i se acordă dreptul să presteze o activitate, pe baza unor reguli, ca urmare a unei proprietăți moștenite din procesul de autentificare.

Pot fi determinate de o gama de restrictii: restricții de timp, restricții de locație fizică, restricții de acces multiplu la resursă etc..

Auditarea reprezintă urmărirea evenimentelor, precum eșecuri de autentificare și autorizare, resurse consumate de către utilizatori.

În afara aspectelor de securitate aceste informații pot fi utilizate pentru management, planificare, facturare etc.

Informațiile tipice strânse conțin identitatea utilizatorului, natura serviciului furnizat, momentul la care serviciul a inceput și când s-a terminat etc.

Metode de autentificare bazate pe un singur factor:

- Autentificare bazată pe ceea ce știi. *Controlul accesului prin parole* - autentificarea cu username și parolă.
- Autentificare bazată pe ceea ce ai. *Controlul accesului prin obiecte* – cartele magnetice, carduri auexpirante, echipamente de identificare personală sau jetoane, PKI și cheia privată.
- Autentificare bazată pe ceea ce ești. *Controlul accesului prin biometrie* – identificările biometrice (amprente digitale, semnătură, voce, forma mîinii, imaginea retinei, imaginea feței etc.
- Autentificare bazată pe locul unde ești. *Controlul geografic al accesului* - autentificarea cu semnatura locației, unde este înregistrat calculatorul, figura 1.

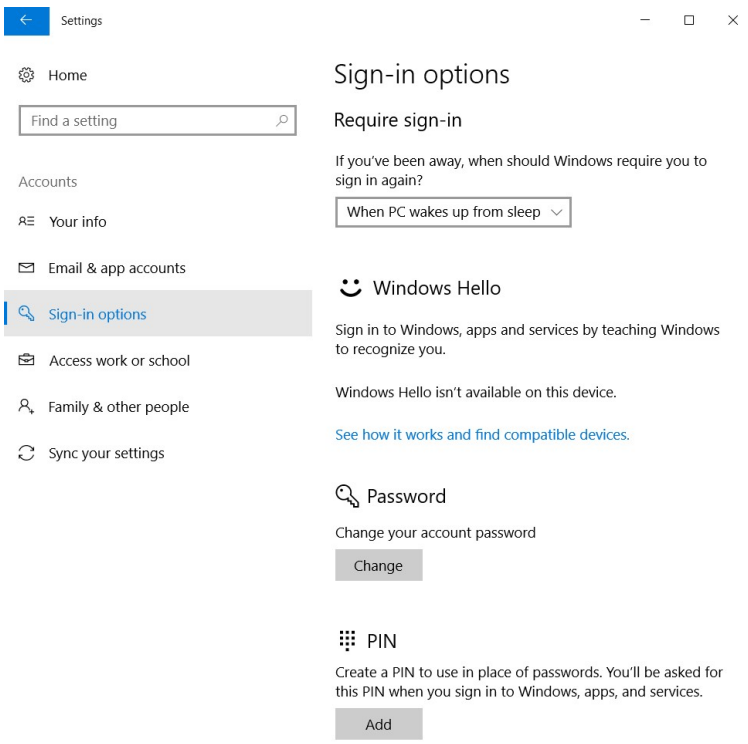

Figura 1. Metode de autentificare în Windows 10

Metode de autentificare bazate pe mai mulți factori (autentificarea multifactorială) sunt metodele de control al accesului care se bazează pe cel puțin două dintre cele 4 căi enumerate (cartelă-parolă, jeton-parolă etc.

Autentificare centralizată: utilizarea unui model centralizat ca autoritate centrală care autentifică utilizatorii remote (la distanță) la un mare număr de sisteme. Utilizează protocoale de autentificare remote ca RADIUS (Remote Access Dial-In User Service), TACACS (Terminal Access Controller Access-Control System), Kerberos, DIAMETER.

Tehnologia one time password (OTP): parola utilizată o singură data, validă doar pentru o singură sesiune de autentificare. Poate fi limitată de un interval de timp și se cere utilizarea tehnologiilor suplimentare (cel mai des telefoanele mobile).

Exemple de OTP: RSA SecurID, utilizatorul poarta un token care este sincronizat în timp cu serverul central RSA.

RISCURI ȘI RECOMANDĂRI

Să fie utilizată autentificarea multifactorială, adică pe lîngă faptul că se utilizează o parolă, să fie utilizat, de exemplu, un mesaj de cod-text de unică folosință, un token de securitat etc.

Să se utilizeze mecanismele de gestiune a parolelor, care asigură autentificarea şi identificarea utilizatorului pentru o perioadă limitată de timp.

2. Managementul parolelor

Parola reprezintă cea mai utilizată metodă de autentificare în sistemele informatice sau servicii web. Din punct de vedere a utilizatorului, memorarea unei parole unice este mai uşor, decît gestionarea mai multora. Pentru atacatori, utilizarea unei singure parole înseamnă că toate sistemele vor fi în mod automat compromise, dacă parola dintr-un sistem slab protejat va fi spartă cu succes.

Parola asigură prima linie de apărare împotriva accesului neautorizat de aceia este esenţial să se mențină eficacitatea acestei linii de apărare implimentîndu-se în mod riguros o bună politică de gestionare şi administrare a parolei.

Pentru un management mai eficient şi menţinerea securităţii parolelor se recomandă respectarea urmatoarelor politici :

- Parola nu trebuie să coincidă cu codul numeric personal, cu data naşterii, cu numărul de telefon, cu nume, prenume, numele de utilizator (login-ul), cu numele membrilor de familiei, cu funcţia, departamentul etc., cu nume de străzi, nume proprii, cu mărci sau modele de maşini etc., cu numele sau sloganul unor organizaţii, să fie termeni tehnici sau cuvinte din dicţionar.
- Parolele nu trebuie comunicate nimănui sub niciun motiv, chiar şi cu scopul reparării calculatorului, în aşa cazuri se creează un cont nou cu un nivel de acces corespunzător.
- Parolele comune trebuie schimbate imediat ce o persoană părăsește grupul sau nu mai are dreptul utilizării.
- Parolele trebuie schimbate imediat ce se constată unele bănuieli privind cunoașterea lor de alte persoane sau compromiterea lor.
- Parolele trebuie ținute minte și nu scrise oriunde (cu excepția necesității intervenției de urgență/plic sigilat).
- Dacă este dificil să se rețină mai multe parole, un manager de parole de încredere poate fi o soluție bună.
- La introducerea parolei nu trebuie să se afle persoane străine prin preajmă.
- Blocarea operațiunilor de încercare repetată de logare.
- Niciodată să nu fie introdusă parola după ce a fost urmat un link dintr-un e-mail primit de la un site care nu prezintă încredere.
- Dacă un terminal funcționează o perioadă lungă de timp, procesul de autentificare trebuie să aibă loc la intervale regulate de timp pentru a se asigura că nu folosește altcineva sistemul.
- La deschiderea unei noi sesiuni de lucru, utilizatorului trebuie să i se aducă la cunoștință ultimul timp de accesare a sistemului cu parola respectivă.
- Evitarea reutilizării parolei anterioare. Dacă un cont de utilizator a fost compromis anterior, fie conștient sau inconștient, reutilizarea parolei ar putea permite compromiterea repetată. Deasemenea, în cazul în care o parolă a fost împărtășită pentru un motiv oarecare, reutilizarea ei ar putea permite cuiva acces neautorizat la conturi.
- Evitarea utilizării aceleași parole pentru mai multe conturi.
- Să nu fie utilizată funcţonalitatea de logare automată. Aceasta diminuează valoarea parolei, dacă un răufăcător va avea acces la un sistem astfel configurat, el va fi în măsură să preia controlul asupra întregului sistem și a avea acces la informații potențial sensibile.
- Notificarea despre schimbarea parolei.
- Actualizarea adresei de e-mail de recuperare în mod regulat, pentru a putea primi e-mailuri în cazul în care este nevoie de resetat parola. De asemenea, se poate adăuga un număr de

telefon pentru a primi codurile de resetare a parolei prin mesaj text. În plus, multe site-uri oferă posibilitatea de a răspunde la o întrebare de securitate în cazul în care parola este uitată. Dacă întrebarea este creată de sinestătător, răspunsul la ea ar trebui să fie cunoscut doar de utilizator. Răspunsul nu ar trebui să poată fi ghicit din informațiile pe care sunt postate online pe bloguri sau pe profilurile din rețelele sociale. Dacă întrebarea este aleasă dintr-o listă de opțiuni, cum ar fi orașul în care v-ați născut, răspunsul trebuie personalizat astfel încît, chiar dacă cineva ghicește răspunsul, nu va ști cum să-l introducă în mod corect.

- Sistemele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parola.

RESTRICȚII

Este interzisă stocarea electronică și transportarea în formă necriptată a parolelor utilizatorilor sistemului, inclusiv a procesului de autentificare a utilizatorilor.

Nu se admite utilizarea în echipamentele și produsele program a parolelor implicite (de la producător).

O parolă puternică reduce riscul ghicirii sau aflării sale prin atacul brute-force. Puterea unei parole este determinată de lungimea, complexitatea şi impredictibilitatea apariţiei caracterelor în componenţa sa.

Pentru crearea unei parole puternice este recomandat ca ea să conţină:

- cel puţin 14 caractere lungime şi nu 8 – ele sunt destul de vulnerabile;
- caractere alfabetice mari și mici (A-Z, a-z);
- cel puțin un caracter numeric (0-9);
- cel puțin un caracter special (~! @ # $% ^ & * () _- + =);
- să poată fi tastată rapid (reduce observarea „peste umăr”).

Modalităţii de creare a parolelor

Există două moduri de creare a parolelor: prin generare aleatoare (sau pseudoaleatoare) şi prin construirea ei de către utilizator.

Generarea aleatoare a parolelor este o metodă recomandată spre utilizare, aplicaţiile de acest tip implimentează recomandările generale pentru crearea unei parole puternice astfel creînd parole indistructibile, dar greu de memorat.

Utilizatorul alege o parola folosindu-se de propria imaginaţie, dar în cele mai multe cazuri acesta utilizează cuvinte întregi din dicţionar sau părţi din acestea, serii de caractere de pe tastatura, adrese, numere de telefon, ani de naştere etc. Deşi sunt uşor de memorat, parolele rezultate sunt şi usor de ghicit, alegerea unor astfel de parole fiind o greşeala mare şi frecventă a utilizatorilor.

Pentru crearea parolelor puternice şi uşor de memorat s-au dezvoltat mai multe metode:

Metoda mnemonicii – se selectează o fraza şi se extrage cîte un caracter din fiecare cuvînt (de exemplu prima sau a doua literă din fiecare cuvînt), apoi se adaugă numere şi simboluri. De exemplu, din fraza *Eu am cea mai puternică parolă vreodată creată de cineva!*, obţinem următoarea parolă: ***Eacmppvcdc!***

Deşi o parolă creată mnemonic este mai puternică decît una creată utilizînd un dicţionar, ele sunt sensibile la atacul brute-force. Frazele uzuale transformate în parole mnemonice, fără folosirea substituții de caractere neobișnuite sau alte modificări, pot fi ghicite de atacatorii utilizându-se dicţionarul parolelor mnemonice. Utilizatorii care creează astfel de parole ar trebui

să creeze propriile fraze, sau să facă schimbări neașteptate, cum ar fi utilizarea caracterilor mari, a semnelor de punctuație, scrierea completă a unor cuvinte.

Modificarea frazelor – se selectează o fraza şi îi se modifică forma într-o derivată de-a sa. Această metodă permite crearea parolelor lungi, complexe şi uşor de memorat. De exemplu, din fraza *to be or not to be* obținem următoarea parolă: ***2.be.0r.nOt@to0.bEE***.

Combinarea şi modificarea cuvintelor - se combină doua sau trei cuvinte fără legătură între ele și se schimbă unele litere cu numere sau caractere speciale. De exemplu, din cuvintele *"mail" and "phone"* obținem următoarea parolă: ***m4!l&f0N3.***

Metoda tiparului - aceasta metodă folosește un tipar (pattern) de pe tastatură. Cu ajutorul tiparului se poate obţine foarte uşor următoarea parolă: ***6VsDrOms;yr***, care de fapt reprezintă *5CaseInalte*. Pentru crearea parolei se selectează de pe tastatura cifra din dreapta la 5, litera din dreapta la "C", litera din dreapta la "a" etc. prin urmare tiparul este selectarea tastei din dreapta pentru fiecare element (figura 2).

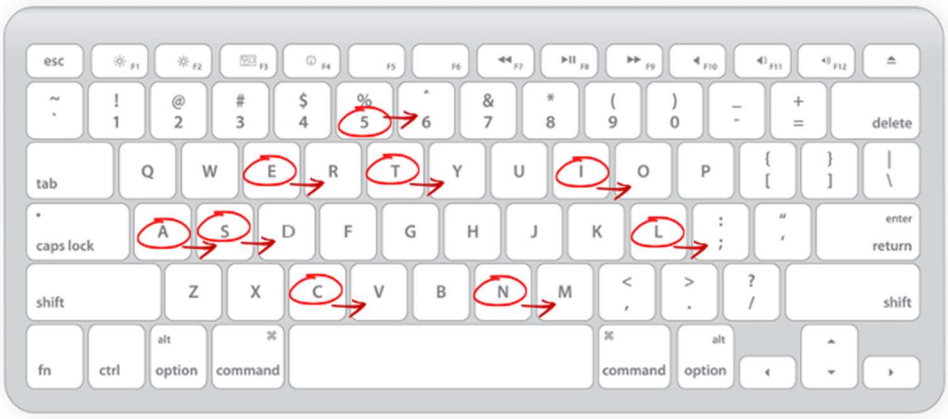

*Figura 2. Metoda tiparului– din **5CaseInalte** obținem parola: **6VsDrOms;yr***

Un alt model de tipar transformă o parola simplă, cu un grad foarte mic de securitate *Avion!*, într-o parolă cu un grad de securitate foarte ridicat ***QWfg8990hj!***" (figura 3).

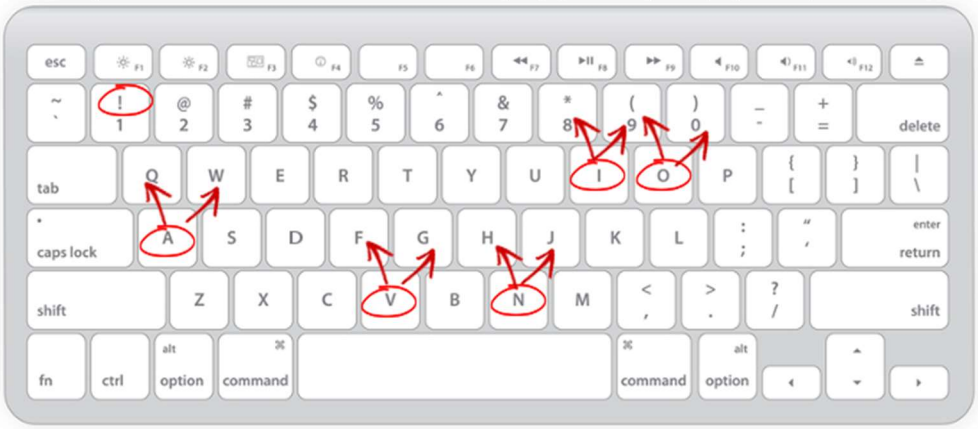

*Figura 3. Metoda tiparului– din **Avion!** obținem parola: **QWfg8990hj!***

2.1.Tehnici de autentificare prin parole

Au fost dezvoltate mai multe soluţii de gestionare şi administrare mai eficientă a parolelor pentru a reduce numărul de conturi şi parole pe care utilizatorii trebuie să le memoreze. Cum ar fi soluţii de management centralizat Single Sign One (SSO), Sincronizarea Parolei şi soluţie de management local - manager de parole. Aceste soluţii reduc probabilitatea compromiterii parolelor deoarece ele nu sunt scrise sau tapate şi dispare necesitatea creării unor parole slabe.

Single Sign One este o tehnologie care permite utilizatorului printr-o singură autentificare să aibă acces la toate resursele la care este autorizat să le utilizeze. Autentificarea la resursele individuale este suportată de către tehnologia SSO într-un mod transparent utilizatorului. Exemple de soluții SSO: Windows Live ID, OpenID.

OpenID este un sistem standard de autentificare a utilizatorilor în cadrul site-urilor. Adică un singur utilizator și o singură parolă poate să se logheze pe toate site-urile fară a mai crea conturi noi sau a confirma email-uri.

Pentru a deține un astfel de cont utilizatorul trebuie sa se inregistreze la un provider OpenId (Google, Facebook, Twitter, Yahoo, Wordpress, LiveJournal, Myspace).

Aceste site-uri nu sunt singurele care oferă un OpenId. Este foarte important ca providerul OpenId-ului să fie unul cît mai sigur şi mai ușor în utilizare.

De obicei site-urile care suportă OpenID pe pagina de autentificare ,pe lîngă cîmpurile standarte login și parolă, au cîmpul OpenID. Pentru a se autentifica utilizatorul trebuie să intoducă în acest cîmp autentificatorul pe care îl primește de la provider-ul Open-ID. Pe lîngă protocolul de autentificare dat se poate folosi și un protocol de autentificare extins. În acest caz utilizatorul creează pe serverul companiei provider un cont cu care se poate loga pe oricare site care suportă OpenID.

Sincronizarea parolei este o soluţie de management care constă în schimbarea parolei la alte resurse cu parola dată de utilizator, astfel el are posibilitatea să se autentifice utilizînd o singură parolă pentru mai multe resurse. Beneficiul principal al acestei soluţii este reducerea numărule de parole pe care utilizatorii au nevoie să și-l amintească. Acest lucru permite utilizatorilor să selecteze parole puternice și să le memoreze mai ușor. Spre deosebire de tehnologia SSO, sincronizarea parolei nu reduce numărul de ori pe care utilizatorii trebuie să se autentifice. Soluția de sincronizare a parolei este de obicei mai ușoară și mai puțin costisitor de implementat decât tehnologiile SSO, dar sincronizarea parolei are și dezavantaje importante de securitate. Deoarece sincronizarea parolei creează aceeași parolă pentru a fi utilizate la mai multe resurse, fiecare dintre care stochează parola sau hash-ul parolei, compromiterea parolei la orice instanță le compromite pe toate. Acest lucru este deosebit de periculos dacă sincronizarea parolei este utilizată pentru resurse cu siguranță înaltă .

O altă abordare a managementului parolelor este un soft de gestionare şi administrare a parolelor.

Managerul de parole este o aplicație software care gestionează și organizează parolele utilizatorului. Softul stochează parole criptate într-o bază de date sau fișier, cerînd utilizatorului să creeze o parolă unică de acces la toată baza de date.

Managerele de parole pot fi folosite ca protecție împotriva phishing-ului și pharming-ului. Spre deosebire de om, softul poate încorpora un script de logare automată, care compară URL-ul site-ului actual cu cel a site-ului stocat, dacă cele două nu se potrivesc, atunci managerul de parole nu completează automat câmpurile de conectare, astfel utilizatorul fiind protejat împotriva imitațiilor vizuale și site-urilor clone. Acest avantaj încorporat, este necesar și utilizatoriilor care memorează cu ușurință parolele.

Majoritatea managelor de parole sunt dotate cu generatoare de parole, oferind utilizatorului posibilitatea creării unor parole indestructibile.

Conform NIST, SP 800-118 Guide to Enterprise Password Management, aplicaţile de management local al parolelor îi sunt recomandate următoarele caracteristici:

- Funcționare: utilizatorul selectează un cont din listă, parola se afișează, utilizatorul o copiază şi o pune în cîmpul parolă.
- Aplicaţia trebuie să se închidă automat după o anumită perioadă de inactivitate.
- Să șteargă automat bufferul de memorie folosit la copierea parolei.
- Să existe posibilitatea de backup a bazei de date şi a informaţiei.
- Să utilizeze o parola Master puternică, greu de ghicit sau spart.
- Să utilizeze algoritmi (şi implementările acestora) aprobaţi de Federal Information Processing Standard (FIPS).
- Utilizatorul trebuie să faca update manual la baza de date dupa fiecare modificare a unei parole.
- Aplicaţia trebuie să permită setarea setului de caractere (cifre, litere mici, mari, simboluri) şi a lungimii pentru fiecare parolă în parte, la alegerea utilizatorului, pentru adaptarea uşoară la diferite sisteme.
- Să poată administra separat parolele cu impact major (importante) de cele normale.
- Să nu permită salvarea de parole şi informaţii sensibile în mod nesecurizat.
- Crearea şi înlocuirea parolelor să se facă uşor pentru facilitarea schimbării periodice.
- La evenimente imprevizibile (crash, etc...) nu trebuie să rămînă parole şi informaţii nesecurizate, pe HDD, SD, Flash sau altă memorie nevolatilă.

Majoritatea managerilor de parolă actualii îndeplinesc aceste caracteristici utilizînd şi caracteristiicii suplimentare cum ar fi logare automată, fără utilizarea tastaturei, aceasta fiind realizată cu ajutorul pluginurilor încorporate în browser-e. Exemplu de manageri de parole: KeePass, eWallet, LastPass, 1Password, RoboForm, Kaspersky Password Manager etc. (figura 4).

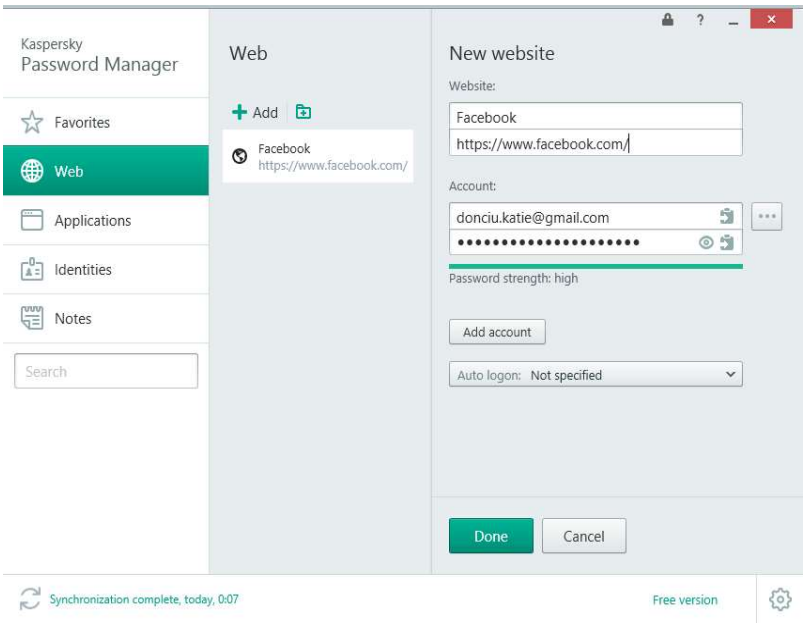

Figura 4. Managerul de parole Kaspersky