Aspecte ale securităţii datelor în spaţiul virtual

Teodora GHERMAN,
doctor în pedagogie, conferenţiar universitar,
Academia de Administrare Publică

Viorel MALCOCI,
master, Academia de Administrare Publică

SUMMARY

This article addresses the subject of the extent of the dangers of the virtual environment and ways to prevent them in the EU Council through the EU Cyber Security Sttrategy. Various methods of secure data management and user accountsare proposed, and formulated requirements for creating secure passwords; introduction to the notion of password generating programs and passwords to access accounts, which can solve problems of data security in cyberspace.

Keywords: EU Cyber Security Sttrategy, secure passwords, password generator, password creation techniques, virtual space.

Introducere. Actualmente, asistăm la o creștere semnificativă a interesului faţă de securitatea informaţională, securitatea Web, dar și a sistemelor hardware. Uniunea Europeană a lansat strategia privind securitäea informatică (EU Cyber Security Sttrategy), elaborată de Chaterine Ashton și Comisia Europeană, care vizează aspecte referitoare la spaţiul virtual. Strategia UE oferă propuneri cu caracter tehnic elaborate de Comisia Europeană (Direcţia Generală Connect) care vor consolida securitatea sistemelor informatice din UE, contribuind, astfel, la sporirea încrederii cetăţenilor care fac cumpărături on-line, ceea ce va contribui la creșterea economică.

În ultimii ani, UE organizează periodic „Luna Securităţii Cibernetice" cu scopul de a spori gradul de conștientizare a securităţii informatice.

Oferirea unui spaţiu cibernetic deschis și securizat este o provocare a timpului pe care UE își propune să o abordeze împreună cu organizaţiile internaţionale relevante și societatea civilă. O colaborare comună privind viziunea globală a Uniunii Europene în domeniul securităţii spaţiului virtual se referă la:

- aplicarea valorilor și drepturilor fundamentale ale UE in spaţiul virtual;
- asumarea responsabilităţii pentru un spaţiu cibernetic deschis, sigur și securizat, care le revine tuturor actorilor societăţii informaţionale globale: de la cetăţeni la administraţiile naţionale;
- consolidarea capacităţilor globale în materie de securitate prin colaborarea UE cu organizaţiile internaţionale, reprezentanţi ai sectorului privat și ai societăţii civile privind sprijinul consolidării capacităţilor terţe, prin înbunătăţirea accesului la informaţii, la un Internet deschis, precum și pentru prevenirea amenintărilor cibernetice.

Strategia în domeniul securităţii cibernetice „Un spaţiu cibernetic deschis, sigur și securizat" reprezintă viziunea globală a UE privind modalităţile de prevenire și gestionare a perturbărilor și atacurilor informaţice.

Strategia UE urmărește scopul de a promova valorile europene referitoare la

libertate şi democraţie, garantarea unei creşteri a economiei digitale în condiţii de siguranţă. Pentru realizarea scopului „este prevăzută o serie de acţiuni specifice care au ca obiectiv creşterea nivelului de rezilienţă a infrastructurilor cibernetice, reducerea criminalităţii informatice şi consolidarea politicii internaţionale a UE în materie de securitate cibernetică şi de apărare împotriva atacurilor cibernetice. [2]

Strategia defineşte cinci priorităţi:

- obţinerea unei rezilienţe a infrastructurilor cibernetice;
- reducerea drastică a criminalităţii informatice;
- dezvoltarea unei politici de apărare împotriva atacurilor cibernetice şi a capacităţilor necesare în contextul politicii de securitate şi apărare comună (PSAC);
- dezvoltarea resurselor industriale şi tehnologice necesare pentru securitatea cibernetică;
- stabilirea unei politici internaţionale coerente a Uniunii Europene privind spaţiul cibernetic şi promovarea valorilor fundamentale ale UE. [2]

Republica Moldova s-a alăturat efortului comun al UE în vederea asigurării securităţii informaţionale. Astfel, au fost elaborate „Recomandări pentru funcţionari" şi „Recomandări pentru cetăţeni" privind securitatea în mediul informatic. [6] Toate aceste măsuri şi practici de combatere a atacurilor informaţionale implementate la nivel mondial arată dimensiunea acestui domeniu, care a luat o amploare deosebită în ultimii ani. [6]

1. Gestionarea conturilor de utilizator. În epoca dezvoltării abundente a reţelelor de socializare, când fără poştă electronică nu-şi imaginează nimeni un proces de business sau o simplă comunicare, o condiţie obligatorie de acces la un serviciu sau la o resursă este setarea unei parole. Activitatea zilnică la calculator, dar mai ales utilizarea Internetului, necesită un număr mare de parole de acces:

- la calculator, telefon etc.;
- la căsuţele poştale;
- la conturile reţelelor de socializare;
- la pagini web;
- la hosting-uri;
- la sisteme de achitări on-line;
- la zone criptate de păstrare a informaţiei etc.

Utilizarea unei singure parole în toate cazurile implică riscuri mari, de aceea vom folosi parole diferite pentru diverse contexte. În majoritatea cazurilor, aceste parole sunt utilizate o dată la 2-3 săptămâni sau chiar mai rar. Câteodată, aceste parole sunt păstrate în aplicaţii specializate de păstrare a parolelor sau în zone criptate la care accesul, de asemenea, se face în baza parolei. Totodată, avem parole care sunt utilizate foarte des. Acestea sunt cele câteva parole care sunt utilizate zilnic pentru a accesa poşta electronică şi contul de pe reţeaua de socializare. În aceste condiţii apare necesitatea ca parolele să fie sigure, să fie logic memorabile şi să fie păstrate doar în memoria utilizatorului.

2. Cerinţe de formare a parolelor sigure. O parolă sigură trebuie:

- să conţină, cel puţin, 8 caractere;
- să conţină caractere din, cel puţin, 3 seturi de caractere de mai jos:

a) literele mici ale alfabetului (a-z);
b) literele mari ale alfabetului (A-Z);
c) cifre (0-9);
d) simboluri speciale (!@#$%^&*()[]?<> ş. a.).

O parolă sigură nu va conţine:

- trei sau mai multe caractere din login;
- cuvinte din dicţionar, slang, dialect, jargon tehnic;
- nu va include numele utilizatorului, nume de persoane, denumiri de localităţi, secvenţe repetate sau secvenţe de tastatură;
- nu va fi scrisă sau stocată on-line;
- nu va fi uşor memorabilă.

Pentru protectia parolelor şi conturilor, nu vom folosi aceeaşi parolă pentru mai

multe conturi. Acest fapt ne oferă următorul beneficiu în cazul în care un cont este compromis, celelalte conturi vor fi în siguranță, nu vor fi supuse riscului de compromitere. În afara riscurilor din mediul virtual, trebuie să ţinem seama de riscurile din mediul real.

Pentru protejarea datelor și păstrarea parolelor:

- nu vom introduce parolele în calculator atunci când cineva poate observa ceea ce tastăm;
- nu vom nota parolele;
- nu vom dezvălui parola nimănui;
- nu vom comunica parola superiorului, managerului, partenerilor, copiilor nostri, prietenilor etc.

Alte consideraţii pentru siguranţa parolelor ţin de următoarele aspecte:

- întotdeauna ieșim (delogăm) sistemele de calcul, sistemele informaţionale sau aplicaţiile, atunci când acestea nu sunt utilizate;
- blocăm calculatorul atunci când nu este utilizat;
- schimbăm imediat parola, dacă bănuim că este cunoscută de către alţii.

Întotdeauna vom ţine minte că, dacă cineva are parola noastră, acesta poate comite acte criminale, folosind contul nostru.

3. Tehnici individuale de formare a parolelor. Pentru a forma o parolă sigură (puternică), putem folosi mai multe tehnici. Putem culege o secvenţă de caractere întâmplătoare de la tastatură în așa mod încât să corespundă cerinţelor de formare a parolelor puternice. Însă în acest caz va fi dificil să reţinem în minte șirul de caractere obţinut.

Formarea parolelor puternice și, totodată, logic memorabile se poate face utilizând tehnici individuale bazate pe fraze logice cunoscute doar utilizatorului. De exemplu: din fraza „În anul 2013 cifra mea norocoasă este 8" putem forma parola „Ia13cmne8." Prin această tehnică pot fi formate parole pentru acces la conturile locale ale utilizatorului.

O altă tehnică este stabilirea de către utilizator a propriului set de caractere pentru formarea parolelor. De exemplu, formăm un set de caractere în care toate vocalele mici ale alfabetului se înlocuiesc cu următoarele simboluri (a – @, e – #, i – !, o – 0(zero), u – ^). Utilizatorul alege unul sau mai multe cuvinte care semnifică ceva important pentru el, presupunem numele „Veronica," formăm parola „V#r0n!c@" sau cuvintele „Zodia Taur" formează parola „Z0d!@T@^r." Parolele formate cu ajutorul acestei tehnici pot fi utilizate pentru accesarea conturilor de poștă electronică, a profilurilor pe reţelele de socializare sau a altor servicii din Internet.

Tehnici de formare a parolelor pot fi inventate la nesfârșit, totul depinde de imaginaţia utilizatorului.

4. Generatoare de parole. O modalitate de a obţine parole cât mai complicate și cât mai greu de ghicit și pentru a fi cât mai siguri că datele nu vor fi compromise, este utilizarea generatoarelor de parole. În continuare, sunt descrise câteva generatoare de parole pentru securizarea conturilor locale, conturilor în Internet sau pentru securitatea dispozitivelor.

Strong Password Generator [10] care poate crea parole cu lungimea de până la 100 caractere. Un avantaj al acestei aplicaţii este oferirea unei modalităţi de memorare mai ușoară a parolei. De exemplu, pentru parola generată „2ok1Q6R1" aplicaţia propune o astfel de pronunţare fonetică „2 oscar kilo 1 QUEBEC 6 ROMEO 1," pentru a fi mai ușor de memorat.

Secure Password Generator [7] care poate crea parole de până la 64 caractere. De asemenea, posedă mecanismul de pronunţare fonetică, iar pentru utilizarea versiunii securizate există posibilitatea utilizării protocolului SSL.

Free Password Generator. [8] Este o aplicaţie relativ simplă care permite generarea

parolelor de lungimi mari de peste 100 caractere.

Random Key Generator. [9] Un site foarte simplu, însă care generează concomitent parole pentru mai multe tipuri de conturi în funcţie de gradul de securizare a acestora, cum ar fi parole pentru conturi locale de acces la calculator, parole de acces la web hosting, parole root sau de administrator.

Utilizarea generatoarelor de parole este raţională în cazul parolelor pentru conturile root sau administrator folosite pentru administrarea serverelor sau a sistemelor informatice sensibile.

5. Parole de acces la conturi. Pentru accesarea sistemelor informatice și a diferitelor resurse din reţeaua Internet, putem deosebi următoarele tipuri de conturi ale utilizatorului:

- conturi locale;
- conturi în Internet;
- conturi de administrare a sistemelor.

Respectiv, în funcţie de importanţa contului, de vulnerabilitatea mediului la care se face acces, de ameninţările asupra sistemelor, se setează şi parolele la aceste conturi.

În cazul accesului la dispozitive separate sau la conturile locale ale sistemului, de operarea vulnerabilităţii acestor sisteme în mare parte depinde de securitatea fizică a echipamentelor.

BIBLIOGRAFIE

1. Planul UE în domeniul securităţii cibernetice pentru protejarea internetului deschis, a libertăţii on-line şi a oportunităţilor generate de internet, Bruxelles, 2013.

2. EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive, <*http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security*>.

3. Remarks by EU High Representative Catherine Ashton at press conference on the launch of the EU's Cyber Security Strategy.

4. Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and informationsecurity across the Union, Brussels, 2013.

5. <*http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm*>.

6. <*http://egov.md/index.php/ro/resurse/securitatea-cibernetica/recomandari-pentru-functionari#.U2ob2YGSxBE*>.

7. <*http://www.pctools.com*>.

8. <*http://www.freepasswordgenerator.com/*>.

9. <*http://randomkeygen.com*>.

10. <*http://strongpasswordgenerator.com/*>.

Prezentat: 7 mai 2014.

E-mail: gherman.teodora@gmail.com