STUDIA UNIVERSITATIS PETRU MAIOR, SERIES OECONOMICA, FASCICULUS 1,
ISSN – L 1843-1127, ISSN 2286-3249 (ONLINE), ISSN 2286-3230 (CD-ROM)

Studiul problemelor de securitate cibernetică

Ioan RUS[1*]

[1] *"Petru Maior" University, Tîrgu Mureș, Nicolae Iorga,no.1, Tîrgu Mureș, 540088, Romania*

Rezumat: *Lucrarea abordează o problematică deosebit de actuală, sensibilă şi periculoasă, securitatea informatică. Autorul defineşte aria de cuprindere, conceptele utilizate, modalităţile de apariţie şi de prevenire a atacurilor informatice. În lucrare sunt prezentate conceptele de securitate a produselor informatice, a reţelelor de calculatoare, securitate informatică şi securitate cibernetică. Deasemenea sunt prezentate modalităţile de apariţie şi de prevenire a atacurilor informatice la nivelul reţelelor de calculatoare, a serverelor de WEB şi a staţiilor de lucru. Un aspect deosebit de important, în acest context, este folosirea echipamentelor mobile şi accesarea reţelelor proprii de la distanţă. În finalul lucrării se identifică câteva modalităţi de prevenire a atacurilor informatice, autorul subliniind rolul factorului uman în implementarea măsurilor de securitate informatică.*

Cuvinte cheie: *informatică, securitate, cibernetică, măsuri de securitate informatică, securitate software.*

Clasificare JEL: O32, O33, C82, C88

[*] *Autorul indicat pentru corespondență: Ioan RUS, tel./fax/ :+40722342787,*
e-mail: irus@artelecom.net

1. INTRODUCERE

Lucrarea are mai multe obiective, printre care: clarificarea conceptului de securitate informatică, sensibilizarea utilizatorilor cu privire la pericolele iminente determinate de atacurile informatice, identificarea punctelor vulnerabile din punct de vedere al atacurilor informatice şi identificarea unor măsuri de prevenire a acestor atacuri. Aşa cum am arătat şi în lucrările mele anterioare [Rus I., 2015], datorită ritmului foarte alert de dezvoltare a tehnologiei informației se modifică concepte și procese economice, se transferă la distanță activități și modalități de prelucrare și/sau stocare a datelor (ca exemplu amintesc apariția conceptului de Cloud Computing), se discută și au devenit legale documentele fără ștampilă, documente în format electronic, documente cu semnătură electronică care sunt echivalente în fața legii cu documentele originale în formă olografă, etc. Constatăm o diversificare foarte mare a echipamentelor mobile care devin componente ale sistemelor informatice (POS, TOKEN-uri, terminale mobile pentru culegea datelor, cititoare de coduri de bare, parole de acces pe telefonul mobil, CARD-uri bancare contactless, etc.) şi o pătrundere generalizată a componentelor electronice programabile în aproape toate tipurile de echipamente de la cele de uz casnic, la maţini fără şofer, drone sau roboţi.

Toate aceste procese, echipamente şi programe culeg, stochează, prelucrează sau răspândesc date de diferite tipuri şi cu grade diferite de confidenţialitate. Protecţia şi controlul acestor date a fost totdeauna o preocupare importantă a celor care le gestionează. În paralel cu această preocupare există şi interesul, uneori major, al altor persoane sau structuri organizaţionale pentru a accesa, stoca sau folosi aceste date. Această ultimă acţiune a unor persoane de a accesa date care nu le aparţin constituie un atentat la securitatea informatică.

Tentaţia de a folosi date sau de a răspândi informaţii cu anumite scopuri, motivate psihologic, a devenit atât de mare, de practică şi de folosită încât vorbim în ultimii 2-3 ani despre o componentă informatică şi informaţională a războaielor neconvenţionale sau a proceselor electorale. Această tentaţie a generat acţiuni majore şi tentative de atacuri informatice la nivel global, adică la nivelul statelor sau mai mult al uniunilor de state.

Pentru a sesibiliza utilizatorii există multe organisme naţionale şi internaţionale ;i reglementări, care se ocupă de protecţia datelor personale [http://www.dataprotection.ro/], respectiv de implementarea măsurilor de securitate informatică [http://qtraces.ro/legislatie/7/LEGISLATIE%20SMSI.pdf].

Cele mai cunoscute reglementări şi organisme în domeniul protecţiei datelor personale sunt următoarele:

- LEGE nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor),
- Directiva (UE) 2016/680 referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii.
- Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

În domeniul securităţii informatice există următoarele reglementări legale, mai importante:

- Hotararea de Guvern nr. 271 din 15 mai 2013 pentru aprobarea Strategiei de securitate ciberne-tica a Romaniei si a Planului de actiune la nivel national privind implementarea Siste-mului national de securitate cibernetica
- Legea nr.82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice

2. DEFINIREA PROBLEMEI CERCETATE

Definirea problemei SECURITĂŢII CIBERNETICE presupune clarificarea conceptelor utilizate, descrierea vulnerabilităţilor şi descrierea posibilităţilor de fraudare .

2.1. **Clarificarea conceptelor** în domeniul securităţii informatice:

În domeniul securităţii informatice există mai multe concepte, care diferă în funcţie de obiectul care este vulnerabil informatic şi de dimensiunea economică, socială sau teritorială pe care se poate produce un atac informatic. Mai trebuie subliniat faptul că atacurile informatice sunt făcute de persoane fizice (hackeri), de grupuri de fizice (hackeri) sau de către diferite organizaţii sau organisme camuflate sau clonate sub diferite nume. Aspectul procurării şi utilizării de date în mod fraudulos a determinat definirea a două concepte diferite: criminalitate informatică şi securitate informatică. Criminalitatea informatică se referă la fapte ilegale produse cu ajutorul mijloacelor informatice sau acu ajutorul datelor procurate în mod fraudulos. Securitatea informatică, conceptul care reprezintă obiectul de studiu al acestei lucrări, se referă la stabilirea vulnerabilităţilor şi a măsurilor de prevenire a atacurilor informatice.

Securitatea informatică este mult mai importantă deoarece previne producerea unor pagube. Referitor la securitatea informatică sunt utilizate mai multe concepte. În primul rând există conceptul de securitate informatică şi securitate cibernetică. Delimitarea celor două se face în funcţie de obiectul ţintă şi de dimensiunea zonei atacate, astfel:

Securitatea informatică se referă la protecţia produselor software: programe informatice, aplicaţii informatice, sisteme informatice, date gestionate de către acestea şi reţele informatice. Produsele software pot funcţiona pe o arie bine definită sau pot fi distribuite pe diferite zone geografice.

În funcţie de tipul de software pe care îl protejează există conceptele de:

Securitatea programelor şi aplicaţiilor informatice - se referă la protecţia produselor software de aplicaţie, care rezolvă problemele utilizatorilor şi la mecanismele de securitate pe care proiectanţii le-au implementat în realizarea acestora;

Securitatea sistemelor informatice – se referă mecanisme de securitate implementate la nielul sistemelor de operare, a programelor utilitare (Office, browse-re, etc), inclusiv a produselor software de aplicaţie ;

Securitatea datelor – se referă la ansamblul mijloacelor de securitate care protejează datele prin tehnica criptării sau a unor mecanisme speciale cum este PGP (Pretty Good Privacy) pentru corespondenţa electronică [**Philip R. Zimmermann,** 2007];

Securitatea reţelelor informatice – se referă la modalităţi de control al utilizatorilor din reţeaua de calculatoare, protecţia identităţii calculatoarelor şi criptarea

mesajelor . Controlul accesului utilizatorilor se face cu regula celor 3 de A, adica AAA (Autentificare, Autorizare, Accounting). Pentru protecţia identităţii folosind protocoale specializate (IPsec, Generic Routing Incapsulation, etc.)

Securitatea cibernetică este un concept global, mai larg, care se referă la protecţia tuturor echipamentelor electronice, componentelor software a datelor şi informaţiilor dintr-un anumit domeniu numit sistem ţintă. Securitatea cibernetică este un concept care include securitatea informatică şi care se extinde în zona echipamentelor mobile, a echipamentelor inteligente şi asupra informaţiilor gestionate de acestea. Informaţiile gestionate de către aceste sisteme se referă şi la datele care nu sunt procesate cu ajutorul calculatoarelor electronice ci reprezintă comunicaţii, imagini, înregistrări online, inclusiv datele procesate de produsele software.

2.2. **Descrierea vulnerabilităţilor**

Vulnerabilitate în conceptul securităţii cibernetice este orice mijloc hardware sau software prin care sistemele informatice sau electronice pot fi accesate sau prin care intră sau ies fluxuri de date. Voi prezenta în acest paragraf descrierea sumară a tipurilor de vulnerabilităţi şi a tipurilor de actori care pot produce atacuri cibernetice. Astfel avem vulnerabilităţi pe diferite nivele ierarhice ale acestor sisteme, după cum urmează :

- Vulnerabilităţi la nivelul echipamentelor mobile şi distante ;
- Vulnerabilităţi la nivelul serverului de acces în sistem ;
- Vulnerabilităţi la nivelul serverul de reţea locală ;
- Vulnerabilităţi la nivelul staţiilor de lucru ;
- Vulnerabilităţi la nivelul programelor de aplicaţie ;
- Vulnerabilităţi la nivelul fuxurilor de date.

La fiecare nivel vulnerabilităţile se concretizează în oportunităţi şi posibilităţi de accesare neautorizată a datelor, programelor sau echipamentelor. Aceste vulnerabilităţi se pot manifesta prin diferite aspecte de comportament ale sistemelor, prin acţiuni sau inacţiuni referitoare la protecţia sistemelor hardware şi software după cum sunt prezentate în continuare.

Vulnerabilităţi la nivelul echipamentelor mobile şi distante : la nivelul echipamentelor mobile vulnerabilitatea de acces se manifestă prin faptul că semnalul de la echipamentul mobil până la intrarea în sistem se realizează prin unde radio la diferite frecvenţe care sunt interceptabile. Deasemenea înstrăinarea, pierderea sau furtul unor astfel de echipamente dacă nu sunt suficient de bine protejate oferă o breşă de vulnerabilitate, mai ales dacă sunt conectabile la sistemele informatice pe care le deservesc.

Vulnerabilităţi la nivelul serverului de acces în sistem : serverul de acces poate fi server de WEB, server de comunicaţii, server de acces la reţeaua locala sau o combinaţie între acestea. Vulnerabilitatea în oricare dintre situaţiile de mai sus este dată de faptul că prin acest punct intră şi ies fluxurile de informaţii spre/dinspre INTERNET. Acest punct de acces poate fi vulnerabil dacă nu sunt implementate serviciile speciale de control acces şi de securitate (SSL- Secure Socket Layer, HTTP - Secure Hypertext. Transfer Protocol, Ipsec, Criptare-Decriptare, etc) . În acest punct de acces vulnerabilităţile cresc dacă se utilizează servicii publice ale INTERNET-ului (corespondenţă electronică publică @yahoo.com ; @gmail.com, etc. ; Facebook ; WhatsApp; QQ – (China); QZone – (China); Instagram; Twitter; Skype; Viber, etc).

Vulnerabilităţi la nivelul serverul de reţea locală – acest server gestionează toată activitatea reţelei proprii de calculatoare, numită şi reţea locală. La nivelul acestui server are loc autentificarea, autorizarea şi accounting-ul utilizatorilor. Gestionarea necorespunzătoare a conturilor de utilizatori şi parole, neimplementarea serviciului de Audit Retail sau necontrolarea fluxurilor de utilizatori prin nodurile reţelei de calculatoare pot facilita accesul neatorizat al unor utilizatori la anumite resurse (programme, date, echipamente) la care nu au dreptul. Aceşti utilizatori pot fi chiar din INTERNET şi care au fost validaţi şi acceptaţi de serverul de WEB;

Vulnerabilităţi la nivelul staţiilor de lucru – la acest nivel se controleaza suplimentar utilizatorii staţiei respective la nivel de autorizare. Acest control se realizează cu ajutorul sistemului de operare;

Vulnerabilităţi la nivelul programelor de aplicaţie – la nivelul programelor de aplicaţie se pot implementa mecanisme speciale de securitate referitoare la gestiunea persoanelor autorizate, sume de control asupra fluxurilor de date, protectia datelor şi a programelor prin algoritmi de identificare şi control al integrităţii. La acest nivel toate mecanismele de securitate sunt proiectate şi realizate de către programatorii soft-urilor respective;

Vulnerabilităţi la nivelul fuxurilor de date – fluxurile de date sunt vulnerabile datorită migrării acestora în timpul procesării. Pentru protejarea datelor trebuie implementate tabelele rolurilor în concordanţă cu regulile de autentificare a utilizatorilor. Deasemenea este necesară criptarea fluxurilor de date şi utilizarea mijloacelor de control al integrităţii acestora.

2.3. **Descrierea posibilităţilor de fraudare**

Fraudarea sistemelor informatice şi mai nou a fluxurilor de date se realizează prin punctele vulnerabile. Fraudarea înseamnă atacarea sistemului informatic, a echipamentelor electronice şi a fluxurilor de date. Scopul fraudării este foarte diversificat de la încetinirea în funcţionare, distrugerea datelor, dar mai ales obţinerea de datelor pentru manipularea lor în scop concurenţial, strategic, militar sau politic.

Fraudarea sistemelor informatice, a echipamentelor electronice şi a fluxurilor de date se face prinidentificarea şi folosirea unor breşe în sistemul de securitate şi se constituie în activităţi de criminalitate informatică.

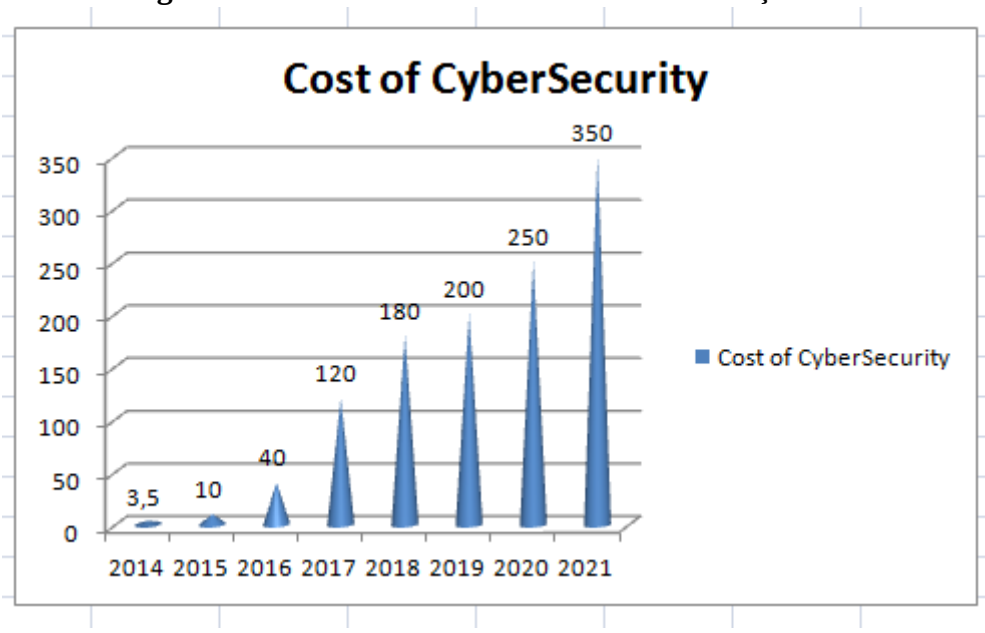
Atacarea sistemelor informatice, a echipamentelor electronice sau a datelor se realizează de către persoane fizice singure sau în grup, organizaţii specializate locale, naţionale, statale sau internaţionale, programe specializate (viruşi, spam-uri, malware, etc) sau echipamente specializate (generatoare de coduri, etc). În ultimii 3 ani se constată o diversificare a fraudelor informatice prin atacarea dispozitivelor mobile sau de securitate, respectiv prin culegerea de informaţii utilizând reţelele de comunicaţii, echipamentele de uz casnic şi chiar echipamentele de comandă şi control electronice instalate pe mijloace AUTO sau în calculatoare de proces ale unor obiective industriale strategice.

În funcţie de scopul urmărit, atacurile informatice sunt orientate pe zone geografice, pe tipuri de afaceri, direct pe unele organizaţii sau state şi mai rar dar cu efecte devastatoare atacuri la nivel planetar.

Studiile de specialitate arată că sumele investite, la nivel mondial, au crescut exponenţial in ultimii 10 – 15 ani şi că această tendinţă se va manifesta în viitor. Astfel un raport, publicat în SUA de Steve Morgan la 31 mai 2017 [https://cybersecurityventures.com/cybersecurity-market-report/] arată care este nivelul costurilor efectuate în domeniul securităţii cibernetice. Potrivit

acestui raport sau cheltuit în domeniul securităţii cibernetice : în anul 2004 suma de 3,5 miliarde de dolari, se estimează că în anul 2017 această sumă va fi de 120 miliarde de dolari, iar în perioada 2017 – 2021 se va cheltui suma suma de 1 trilion de dolari, adică estimativ suma medie de 250 miliarde dolari anual. Acelaşi studiu estimează că în următorii 13 ani cheltuielile din domeniul securităţii cibernetice vor creşte de 35 ori. Odată cu această creştere explozivă a cheltuielilor din domeniul securităţii cibernetice va creşte într-un ritm alert şi necesarul de forţă de muncă calificată (specialişti) în acest domeniu. O reprezentare grafică a costurilor estimate în domeniul securităţii cibernetice este prezentat în fig. nr.1.

Figura nr. 1. – Cheltuieli în domeniul Securităţii Cibernetice



*Sursa: Proiecţia autorului, pe baza datelor din [*https://cybersecurityventures.com/cybersecurity-market-report/*]*

3. MĂSURI pentru CREŞTEREA nivelului de SECURITATE CIBERNETICĂ

Dimensiunea, frecvenţa şi ritmul accelerat de dezvoltare a criminalităţii informatice determină utlizatorii (persoanele fizice, organizaţiile şi statele) să întreprindă cât mai repede măsuri şi strategii de prevenire a atacurilor informatice.

Informaţiile şi datele circulă în INTERNET cu o viteză foarte mare şi cu o dispersie uimitoare. Acesarea unui singur server din INTERNET poate difuza mesajul în zeci sau sute de puncte din INTERNET, depinde de mulţimea şi interesul celor care iau contact cu mesajul. Punctele de vulnerabilitate a securităţii cibernetice sunt atacate în majoritatea cazurilor din INTERNET sau prin conexiunea la INTERNET.

Trebuie să menţionez faptul că măsurile de securitate cibernetică care vor fi prezentate mai jos NU înlocuiesc şi NU exclud măsurile de protecţie şi fiabilitate a sistemelor informatice.

În acest context măsurile de securitate cibernetică, după părerea mea, pot fi de două feluri:

Obişnuite – în cazul în care organizaţia doreşte să stabilească un raport între daune posibile, măsuri de securitate informatică şi riscul asumat.

Radicale – în cazul în care organizaţia are date extrem de sensibile pe care doreşte cu orice preţ să le protejeze.

Măsurile obişnuite de securitate derivă din vulnerabilităţile sistemului şi din modul de manifestare al acestora. Amploarea măsurilor de securitate cibernetică depind de dimesiunea, aria de răspândire şi nivelul de protecţie dorit. Un aspect foarte important, semnalat, cu ocazia diferitelor manifestări ştiinţifice din acest domeniu [Stănescu R., 2017] este rolul factorului uman în implementarea măsurilor de securitate informatică. Dispozitivele mobile, token-urile, cheile de acces sunt în mâna utilizatorilor. Oricâte măsuri de securitate ar fi luate dacă utilizatorii nu conştientizează şi nu aplică măsurile de securitate cibernetică impuse vulnerabilităţile devin tot mai evidente, chiar se produc breşe deschise în securitatea informatică. Pentru a fi mai explicit dau un singur exemplu foarte simplu: o persoană care foloseşte servicile de INTERNET BANKIG de pe telefonul mobil are configurate, salvate şi setate toate datele de acces la acest serviciu. Conectarea şi accesul se realizează printr-un singur click pe o pictogramă pe care scrie „Plăţi_OnLine". Persoana respectivă îşi pierde telefonul mobil. Probabilitatea ca cel care-l găseşte să poată să facă viramente în alte conturi este foarte mare. După efectuarea plăţilor aruncă telefonul sau chiar îl duce undeva în zona în care proprietarul să-l poată recupera. Este foarte greu, aproape imposibil să produci probe credibile şi să identifici autorul fraudei în asemenea cazuri (mai ales dacă nici probele video nu mai pot fi utilizate).

În mod standard măsurile de securitate cibernetică cuprind un complex de acţiuni, echipamente, programe şi strategii de natură specifică. Ce trebuie să facem concret sintetiza domnul Cătălin Pătraşcu – reprezentantul Centrului Naţional de Răspuns la incidente de securitate cibernetică (CERT) la ultima Conferinţă Naţională în domeniul securităţii cibernetice [Pătraşcu C., 2017]. Cele mai importante măsuri de securitate, după părerea domnului Cătălin Pătraşcu, sunt următoarele, citez [Pătraşcu C., 2017]:

1. „Securitatea terminalelor (antimalware, firewall, DLP, OS modern, actualizări regulate, criptare);
2. Atenție sporită la BYOD; (*utilizarea echipmentelor personale la serviciu)*
3. Securitatea rețelei (segmentare, NGFW, SIEM);
4. Vizibilitate (SOC);
5. Restricționarea accesului utilizatorilor (principiul need to know) ;
6. Politică de backup (testat în mod regulat);
7. Politică de securitate (luată la cunoștință de utilizatori, impusă);
8. Managementul incidentelor și al vulnerabilităților;
9. Audituri regulate de securitate cibernetică și evaluări de securitate (pentest);
10. Personal bine pregătit și conștient de pericolele cibernetice."

Fiecare entitate organizatorică va stabili care este nivelul de securitate informatică dorit şi care sunt costurile pe care le este dispusă să le suporte pentru implementarea măsurilor de securitate cibernetică.

Măsurile radicale se pot concretiza prin inchiderea totală a accesului la INTERNET. Prima reacţie a utilizatorilor ar fi aceea că NU se poate fără INTERNET, ceea ce este corect şi adevărat. Acest tip de măsuri se realizează prin utilizarea unui INTRANET fără acces la INTERNET, având ca suport un VPN propriu şi realizarea unui alt VPN prin care se asigură accesul la INTERNET. In acest context este indicat ca sistemele de operare folosite să fie din categoria celor mai puţin vulnerabile la atacuri informatice. Este cunoscut faptul că sistemul de

operare WINDOWS este cel mai expus la asemenea atacuri mai ales datorită răspândirii lui pe foarte multe calculatoare, echipamente mobile şi alte echipamente electronice.

4. CONCLUZII

Într-o scurtă perioadă de timp, cca. 5 ani, securitatea cibernetică a devenit o problemă de interes mondial, deosebit de importantă şi de periculoasă. Organismele naţionale şi internaţionale includ securitatea cibernetică ca o componentă a strategiilor de securitate naţională sau internaţională. În urma studiului de mai sus am ajuns la următoarele concluzii:

1.) înregistrarea şi manipularea unui volum foarte mare de date şi informaţii, alături de facilităţile oferite de INTERNET au atras interesul unor persoane sau organizaţii de a le prelua în mod fraudulos şi de a le folosi în lupta mondială pentru putere şi supremaţie ;
2.) organizaţiile trebuie să conştientizeze acest fenomen şi să-şi construiască propia strategie de securitate informatică.
3.) auditarea sistemelor informatice va deveni din ce în ce mai mult o componentă a strategiei de securitate informatică ;
4.) resursa umană (utilizatorii individual sau în organizaţii) sunt şi vor reprezenta un element hotărâtor în descrierea şi implementarea strategiei de securitate informatică.
5.) trebuie organizate cât mai multe acţiuni pentru conştientizarea personală a vulnerabilităţilor securităţii cibernetice, respectiv a pericolelor criminalităţii cibernetice (conferinţe, instruiri, cursuri, certificări de competenţe, etc).

Bibliografie:

Pătraşcu Cătălin - *Conformitate vs Securitate în contextul GDPR şi al Directivei NIS, ,* la Conferinţa Naţională în domeniul securităţii cibernetice, Bucureşti, 2017, *virtual ref:* http://isaca.ro/wp-content/uploads/2017/12/Catalin-Patrascu-_-CERT-RO_ISACA_BNR_08.12.2017.pdf

Philip R. Zimmermann - *The Official PGP User's Guide*, Publisher MIT Press, 1995, 2007, Michigan, 127 pages, ISBN: 0262740176, 9780262740173, virtual ref: https://books.google.ro/books/about/The_Official_PGP_User_s_Guide.html?id=dP1SAAAAMAAJ&redir_esc=y

Rus, I., - *Technologies and Methods for Auditing Databases*- în revista Procedia Economics and Finance, nr.26/2015, pag. 991-999, Publisher: ELSEVIER, ISSN: 2212-5671;

Stănescu Radu – *Vulnerabilitatea umană în securitate cibernetică*, la Conferinţa Naţională în domeniul securităţii cibernetice, Bucureşti, 2017, *virtual ref:* http://isaca.ro/wp-content/uploads/2017/12/Radu-Stanescu-Human-Vulnerability-in-Cybersecurity.pdf

Virtual references :

http://www.dataprotection.ro/

http://qtraces.ro/legislatie/7/LEGISLATIE%20SMSI.pdf

https://cybersecurityventures.com/cybersecurity-market-report/

http://isaca.ro/wp-content/uploads/2017/12/Catalin-Patrascu-_-CERT-RO_ISACA_BNR_08.12.2017.pdf

STUDIA UNIVERSITATIS PETRU MAIOR, SERIES OECONOMICA, FASCICULUS 1,
ISSN – L 1843-1127, ISSN 2286-3249 (ONLINE), ISSN 2286-3230 (CD-ROM)

Study of cybersecurity issues

Ioan RUS[1†]

[1] *"Petru Maior" University, Tîrgu Mureș, Nicolae Iorga,no.1, Tîrgu Mureș, 540088, Romania*

Abstract: *The paper addresses a particularly current, sensitive and dangerous problem, computer security. The author defines the scope, concepts used, ways of appearing and preventing computer attacks. The paper presents the concepts of security of computer products, computer networks, cyber security and cyber security. Also, there are presented the ways of occurrence and prevention of computer attacks at the level of computer networks, WEB servers and workstations. An especially important aspect in this context is the use of mobile devices and access to remote networks. At the end of the paper several ways to prevent computer attacks are identified, the author stressing the role of the human factor in the implementation of IT security measures.*

Keywords: *software, information technology, security, cybernetics, IT security measures, software security.*

JEL Classification: O32, O33, C82, C88

[†] Corresponding author*: Ioan RUS, tel./fax/ :+40722342787,*
e-mail: irus@artelecom.net

1. INTRODUCTION

The work has several goals, including: clarifying the concept of computer security, raising awareness of the imminent threats posed by cyber attacks, identifying vulnerabilities from the point of view of cyber attacks, and identifying measures to prevent these attacks. As I have shown in my earlier works [Rus I., 2015], due to the very rapid pace of development of information technology, economic concepts and processes are changed, remote data transfer and / or processing and / or storage example recall the emergence of the Cloud Computing concept), documents without stamps, electronic documents, electronic signature documents that are equivalent before the law with the original hand-made documents, etc. are discussed and made legal. We find a great deal of diversification of mobile devices becoming components of computer systems (POS, TOKENs, mobile data collection terminals, barcode readers, mobile access passwords, contactless bank cards, etc.) and a generalized penetration of programmable electronic components in almost all types of equipment from household, to machine-driven machines, drones or robots.

All these processes, equipment and programs collect, store, process or disseminate data of different types and with different degrees of confidentiality. The protection and control of these data has always been an important concern for those who manage them. In addition to this concern, there is also the interest, sometimes major, of other people or organizational structures to access, store or use these data. This last action of some people to access data that does not belong to them is a computer security attack.

The temptation to use data or to spread psychologically motivated information has become so great, practical and useful that we have been talking about an informational and informational component of unconventional wars or electoral processes over the past 2-3 years. This temptation has generated major actions and attempts at cyber-attacks worldwide, ie at the level of states or more of the unions of states.

In order to inform users, there are many national and international bodies and regulations that deal with the protection of personal data [http://www.dataprotection.ro/], respectively the implementation of IT security measures [http://qtraces.ro/ legislation / 7 / LEGISLATION% 20SMSI.pdf].

The most common regulations and bodies in the field of personal data protection are as follows:

- LAW no. 677 of 21 November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data;
- Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Directive),
- Directive (EU) 2016/680 on the protection of personal data in specific activities carried out by law enforcement authorities.
- National Authority for the Supervision of Personal Data Processing.

In the field of IT security, there are the following more important legal regulations:

- Government Decision no. 271 of 15 May 2013 for the approval of the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System
- Law no.82 / 2012 on the retention of data generated or processed by the providers of public electronic communications networks and the providers of

publicly available electronic communications services, as well as for amending and completing the Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector

2. PROBLEM DEFINITION INVESTIGATED

Defining the CIBERSECURITY problem involves clarifying the concepts used, describing the vulnerabilities and describing the possibilities of fraud.

2. 1. **Clarification of concepts** in the field of IT security:

In the field of IT security, there are several concepts that differ according to the object that is vulnerable to computer and the economic, social or territorial dimension on which an IT attack may occur. It should also be emphasized that computer attacks are made by individuals (hackers), by groups of physicists (hackers) or by various organizations or bodies camouflaged or cloned under different names. The appearance of fraudulent procurement and use of data has led to the definition of two different concepts: cybercrime and computer security. Cybercrime refers to illicit deeds produced by means of information technology or to the use of data fraudulently obtained. Computer security, the concept that is the subject of this study, refers to the identification of vulnerabilities and measures to prevent cyber attacks.

Computer security is more important because it prevents damage. In terms of computer security, several concepts are used. First there is the concept of computer security and cyber security. The delimitation of the two is based on the target object and the size of the attacked area, as follows:

Computer security refers to the protection of software products: software, computer applications, information systems, data managed by them and computer networks. Software products can operate on a well-defined area or can be distributed across different geographic areas.

Depending on the type of software they are protecting, there are the concepts of:

Security of software and applications - refers to the protection of application software products, which solves users' problems and the security mechanisms that the designers have implemented in their implementation;

Information Systems Security - refers to security mechanisms implemented at the operating systems, utility programs (Office, browse-re, etc.), including application software products;

Data Security - refers to all the security features that protect data through encryption techniques or special mechanisms such as PGP (Pretty Good Privacy) for electronic mail [Philip R. Zimmermann, 2007];

Computer Network Security - refers to ways to control users on the computer network, protect computer identity, and encrypt messages. User access control is done with the 3 A rule, ie AAA (Authentication, Authorization, Accounting). For identity protection using specialized protocols (IPsec, Generic Routing Incapsulation, etc.).

Cybersecurity is a broader, broader concept that covers the protection of all electronic equipment, software components of data and information in a particular domain called a target system. Cybersecurity is a concept that includes information security and extends to mobile

equipment, intelligent equipment and the information it manages. The information managed by these systems also covers data that is not processed by electronic computers but represents communications, images, online records, including data processed by software products.

2. 2. **Vulnerability description**

Vulnerability in the concept of cyber security is any hardware or software through which computer or electronic systems can be accessed or through which data streams or data come in or out. I will present in this paragraph the brief description of the types of vulnerabilities and the types of actors that can cause cyber attacks. So we have vulnerabilities on different hierarchical levels of these systems as follows:

- Vulnerabilities in mobile equipment and distances;
- Vulnerabilities in the system access server;
- Vulnerabilities at the local network server level;
- Vulnerabilities at the workstations;
- Vulnerabilities in application programs;
- Vulnerabilities in data fuses.

At each level vulnerabilities materialize in opportunities and possibilities of unauthorized access to data, programs or equipment. These vulnerabilities can be manifested through different behavioral aspects of systems, by actions or inactions related to the protection of hardware and software systems as outlined below.

Vulnerabilities in mobile equipment and distances: At the level of mobile equipment, the vulnerability of access is manifested by the fact that the signal from the mobile equipment to the system entry is realized by radio waves at different frequencies that are interceptable. Also, the alienation, loss or theft of such equipment if not adequately protected provides a breach of vulnerability, especially if they are connectable to the computer systems they serve.

Vulnerabilities at the system access server: The access server can be a WEB server, a communications server, a local network access server, or a combination of these. Vulnerability in any of the above situations is due to the fact that through this point the information flows to and from the INTERNET. This access point may be vulnerable if special access and security control services (SSL-Secure Socket Layer, HTTP, Secure Hypertext, Transfer Protocol, Ipsec, Encrypt-Decryption, etc.) are not implemented. At this access point, vulnerabilities grow if public Internet services are used (public e-mail @ yahoo.com; @ gmail.com, etc; Facebook; WhatsApp; QQ - (China); QZone - (China); Instagram , Twitter, Skype, Viber, etc.).

Vulnerabilities at the local network server level - this server manages all the activity of your own computer network, also called a local network. Server authentication, authorization, and accounting are made at this server level. Inappropriate management of user accounts and passwords, non-implementation of Audit Retail, or non-control of user flows through computer nodes may facilitate unauthorized access to certain resources (programs, data, equipment) to which they are not entitled. These users can even be on the INTERNET and have been validated and accepted by the WEB server;

Vulnerabilities at the workstations - at this level, the users of the respective station at the authorization level are additionally controlled. This control is done with the operating system;

Application-level vulnerabilities - Special security mechanisms for managing authorized persons, checksums on data flows, data protection, and programs through integrity identification and control algorithms can be implemented at application program level. At this level, all security mechanisms are designed and built by programmers of the respective software;

Vulnerabilities at Data Streams - data streams are vulnerable due to migration during processing. To protect data, roles tables must be implemented in accordance with user authentication rules. It is also necessary to encrypt data streams and use the means to control their integrity.

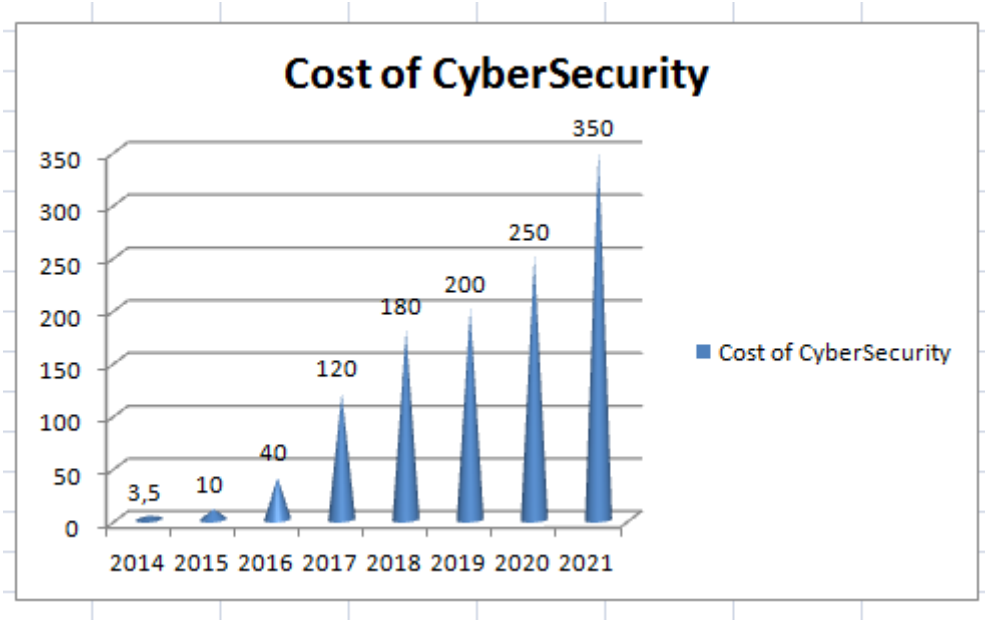
2.3. Description of fraud possibilities

Fraud of information systems and newer data streams is done through vulnerabilities. Fraudation means attacking the computer system, electronic equipment and data streams. The purpose of fraud is very diversified from slowing down, destroying data, but especially getting data for manipulation for competitive, strategic, military, or political purposes.

Fraudation of computer systems, electronic equipment and data flows is made through the identification and use of breaches in the security system and constitutes crime cybercrime activities.

The attack of computer systems, electronic equipment or data is carried out by individuals or groups, specialized local, national, state or international organizations, specialized programs (viruses, spam, malware, etc.) or specialized equipment codes, etc.). Over the past 3 years, there has been a diversification of computer fraud by attacking mobile or security devices, or by gathering information using communications networks, household equipment, and even electronic control and control equipment installed on AUTO means or in process computers of strategic industrial objectives.

Figure no. 1. - Expenditure in the field of CyberSecurity



Source: Author's proposal based on [https://cybersecurityventures.com/cybersecurity-market-report/]

Depending on the purpose, the attacks are targeted geographically, by business type, directly on some organizations or states, and more rarely, but with devastating effects on a planetary level.

Specialist studies show that the amounts invested worldwide have increased exponentially in the last 10-15 years and that this trend will be manifested in the future. Such a report, published in the US by Steve Morgan on May 31, 2017, [https://cybersecurityventures.com/cybersecurity-market-report/], shows the level of costs involved in cyber security. According to this report or spent in the field of cyber security: in 2004 the amount of 3.5 billion dollars, it is estimated that in 2017 this amount will be 120 billion dollars, and in the period 2017 - 2021 will spend the sum amount 1 trillion dollars, that is, an estimated average of $ 250 billion annually. The same study estimates that over the next 13 years, cyber security spending will increase 35 times. With this explosive growth in cyber security spending, the need for skilled labor (specialists) in this area will grow at a rapid pace. A graphical representation of estimated costs in the field of cybersecurity is shown in Fig. no. 1.

3. ACTIONS TO INCREASE THE CYBERSECURITY LEVEL

The speed, frequency, and accelerated rate of cybercrime development determines the users (individuals, organizations, and states) to take measures and strategies to prevent cyber attacks as soon as possible.

Information and data circulate on the Internet at a very high speed and with amazing dispersion. Having a single INTERNET server can broadcast the message in tens or hundreds of INTERNET points depends on the crowd and interest of those who are in contact with the message. Cyber security vulnerabilities are attacked in most cases on the INTERNET or through the Internet connection.

I must mention that the cybersecurity measures that will be presented below DO NOT replace and DO NOT exclude the protection and reliability of information systems.

In this context, cybersecurity measures, in my opinion, can be of two kinds:

Common security measures - if the organization wants to establish a relationship between possible damage, IT security measures and assumed risk.

Radical measures - if the organization has extremely sensitive data that it wishes to protect at any cost.

Common security measures derive from the system's vulnerabilities and how they manifest. The magnitude of cyber security measures depends on the size, spread, and level of protection desired. A very important aspect, pointed out at various scientific manifestations in this field [Stănescu R., 2017] is the role of the human factor in the implementation of IT security measures. Mobile devices, tokens, access keys are in the hands of users. Whatever security measures would be taken if users did not realize and do not apply the cyber security measures imposed on the vulnerabilities become more and more obvious, even open breaches in computer security occur. To be more explicit, I give a very simple example: a person who uses INTERNET BANKIG services on his mobile phone has configured, saved and set all access data to this service. Connecting and accessing is done with a single click on an icon that says "Pay_OnLine". That person loses his cell phone. The likelihood that the person who finds it will be able to make transfers into other accounts is very large. After making payments, he throws the phone or even takes him to the area where the owner can recover it. It is very hard, almost

impossible to produce credible evidence and to identify the author of fraud in such cases (especially if video samples can no longer be used).

Cybersecurity measures typically include a set of actions, equipment, programs and strategies of a specific nature. What do we have to do concretely synthesize Mr. Cătălin Pătraşcu, the representative of the National Center for Cyber Security Incidents Response (CERT) at the last National Conference on Cyber Security (Pătraşcu C., 2017). The most important security measures, according to Mr. Cătălin Pătraşcu, are the following, I quote [Pătraşcu C., 2017]:

1. "Terminal Security (antimalware, firewall, DLP, modern OS, regular updates, encryption);
2. Increased attention to BYOD; (use of personal equipment at work)
3. Network security (segmentation, NGFW, SIEM);
4. Visibility (SOC);
5. Restrict user access (need to know principle);
6. Backup Policy (Regularly Tested);
7. Security policy (user-imposed, imposed);
8. Incident and vulnerability management;
9. Regular cyber security audits and security assessments (pentest);
10. Well-prepared and aware of cyber-dangers. "

Each organizational entity will determine what level of IT security is desired and what costs it is willing to bear for the implementation of cyber security measures.

The radical measures can be concretized by the complete closure of the INTERNET access. The first reaction of users is that it can NOT be without INTERNET, which is correct and true. This type of measures is achieved by using an INTRANET without access to the Internet, supporting a VPN and creating another VPN that provides access to the INTERNET. In this context, it is indicated that the operating systems used are the least vulnerable to computer attacks. It is known that the WINDOWS operating system is most exposed to such attacks, especially due to its spread on many computers, mobile equipment and other electronic equipment.

4. CONCLUSIONS

In a short time, approx. 5 years, cyber security has become a matter of global concern, particularly important and dangerous. National and international bodies include cyber security as a component of national or international security strategies. Following the above study, we came to the following conclusions:

1.) recording and manipulating a huge amount of data and information alongside the facilities offered by INTERNET have attracted the interest of individuals or organizations to take them fraudulently and to use them in the world struggle for power and supremacy;
2.) organizations need to be aware of this phenomenon and build their own IT security strategy ;
3.) computer systems auditing will increasingly become a component of the IT security strategy ;
4.) the human resource (individual users or organizations) is and will be a decisive element in the description and implementation of the IT security strategy;

5.) as much action as possible for personal awareness of the cyber security vulnerabilities and the dangers of cyber crime (conferences, trainings, courses, skills certifications, etc.) should be organized.

Bibliography:

Pătrașcu Cătălin - *Conformitate vs Securitate în contextul GDPR și al Directivei NIS, ,* la Conferința Națională în domeniul securității cibernetice, București, 2017, *virtual ref:* http://isaca.ro/wp-content/uploads/2017/12/Catalin-Patrascu-_-CERT-RO_ISACA_BNR_08.12.2017.pdf

Philip R. Zimmermann - *The Official PGP User's Guide*, Publisher MIT Press, 1995, 2007, Michigan, 127 pages, ISBN: 0262740176, 9780262740173, virtual ref: https://books.google.ro/books/about/The_Official_PGP_User_s_Guide.html?id=dP1SAAAAMAAJ&redir_esc=y

Rus, I., - *Technologies and Methods for Auditing Databases*- în revista Procedia Economics and Finance, nr.26/2015, pag. 991-999, Publisher: ELSEVIER, ISSN: 2212-5671;

Stănescu Radu – *Vulnerabilitatea umană în securitate cibernetică*, la Conferința Națională în domeniul securității cibernetice, București, 2017, *virtual ref:* http://isaca.ro/wp-content/uploads/2017/12/Radu-Stanescu-Human-Vulnerability-in-Cybersecurity.pdf

Virtual references :

http://www.dataprotection.ro/

http://qtraces.ro/legislatie/7/LEGISLATIE%20SMSI.pdf

https://cybersecurityventures.com/cybersecurity-market-report/

http://isaca.ro/wp-content/uploads/2017/12/Catalin-Patrascu-_-CERT-RO_ISACA_BNR_08.12.2017.pdf