LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

Aprob,

Director General al CERT-RO

Augustin JIANU

GHID

de securitate informatică pentru funcționarii publici

- Versiunea 1.1 -

Realizat de către:

BE AWARE, BE SECURE.
www.enisa.europa.eu/cybersecmonth

www.cert.ro/ecsm.php

Pagină albă

Cuprins

Pagină albă

1. Introducere

1.1. Context

Apariţia şi dezvoltarea calculatoarelor electronice a reprezentat o adevărată revoluţie în societatea umană, având ca principală consecinţă tranziţia de la societatea industrială la societatea informaţională.

Calculatorul a devenit o componentă normală a activităţii noastre zilnice, iar tehnologia comunicaţiilor şi posibilităţile oferite de Internet au produs transformări în întreaga societate, pătrunzând în toate aspectele vieţii economice, sociale şi culturale.

Accesul la informaţie prin intermediul Internetului şi, mai ales, abilitatea de a analiza o mare cantitate de date cu ajutorul calculatorului, constituie avantaje fără precedent care, dacă sunt puse la dispoziţia unui număr cât mai mare de indivizi, instituţii, agenţi economici sau administraţii, determină creşterea productivităţii, progresul societăţii şi creşterea calităţii vieţii, în general.

Informaţia este o resursă care are o importanţă deosebită pentru desfășurarea activităților unei instituții şi, în consecinţă, necesită o protecţie adecvată. Informaţiile pot exista sub diferite forme: tipărite sau scrise pe hârtie, stocate electronic, transmise prin poştă sau prin mijloace electronice, prezentate în filme, sau rostite în cadrul unor conversaţii. Orice formă ar avea informațiile și indiferent de mijloacele utilizate pentru a fi distribuite sau stocate, trebuie întotdeauna să fie protejate corespunzător.

Securitatea informațiilor înseamnă protejarea informațiilor față de o gamă largă de amenințări și vulnerabilități pentru a asigura continuitatea activității și reducerea riscului organizațional. Securitatea informaţiilor este obţinută prin implementarea unui set adecvat de măsuri de securitate, incluzând politici, procese, proceduri, structuri organizaţionale, funcționalități software și hardware. Este necesar ca aceste măsuri de securitate să fie stabilite, implementate, monitorizate, revizuite și îmbunătățite, după caz, pentru a se asigura atingerea obiectivelor specifice și de securitate. Angajații din domeniul public sunt responsabili să se asigure că gestionarea datelor și informațiilor sensibile este făcută conform legilor și regulilor aflate în vigoare.

Datorită utilizării extensive în prezent a dispozitivelor mobile, atât pentru uz personal cât și pentru desfășurarea activităților specifice locului de muncă, angajații trebuie să se asigure de faptul că acest proces se desfășoară în concordanță cu politicile și liniile directoare ale instituției angajatoare. Majoritatea datelor prelucrate și stocate de către instituțiile de stat sunt protejate printr-o clasificare de securitate, fiind cel puțin secret de serviciu.

1.2. Scop

Prezentul ghid cuprinde o serie de recomandări cu caracter general menite să îmbunătățească cultura de securitate informatică a funcționarilor publici și să-i familiarizeze pe aceștia cu modul în care ar trebui implementate și folosite tehnicile, instrumentele şi mecanismele de securitate astfel încât să fie asigurată securitatea informației în instituțiile publice.

Ghidul nu trebuie considerat ca fiind exhaustiv, măsurile cuprinse de acesta putând fi considerate ca necesare însă nu neapărat și suficiente.

1.3. Obiective

Ghidul de securitate informatică pentru funcționarii publici îşi propune următoarele obiective:

- creșterea confidenţialităţii, integrităţii şi disponibilităţii datelor şi informaţiilor vehiculate în cadrul sistemelor informatice şi de comunicaţii utilizate de funcționarii publici;
- oferirea mijloacelor de ghidare şi susţinere a activităţii referitoare la securitatea informaţiei în cadrul instituțiilor, prin definirea de controale şi măsuri ce vizează identificarea și reducerea riscurilor şi vulnerabilităţilor de securitate manifestate în cadrul acestora;
- creșterea nivelului general de cunoștințe în domeniul securității cibernetice al funcționarilor publici, în scopul îmbunătățirii climatului general de securitate cibernetica în instituțiile publice;
- promovarea elaborării, de către compartimentele IT specializate din instituțiile publice, a unor ghiduri, sau manuale de utilizare a echipamentelor de calcul în interiorul, sau în interesul instituțiilor publice respective.

2. Reguli de securitate informatică

În rândurile următoare se regăsesc câteva reguli generale de utilizare a dispozitivelor de calcul la locul de muncă sau care aparțin instituției unde vă desfășurați activitatea:

- Utilizați echipamentele de calcul de serviciu în scop profesional, de serviciu;
- Instalați pe echipamentele de calcul de serviciu numai aplicații utilizate în scop profesional, de serviciu. Preferabil, utilizați pe echipamentele de calcul de serviciu numai aplicații software validate de către compartimentul IT al instituției dumneavoastră;
- Instalați pe echipamentele de calcul de serviciu numai aplicații cu licență validă (comercială, gratuită sau cu sursă deschisă) și care provin numai din surse sigure, verificabile de către compartimentele IT ale instituției dumneavoastră;

- Utilizați echipamentele de calcul în scop profesional, de serviciu, numai în locații în care riscul de efracție și delapidare este foarte redus;
- Nu lăsați niciodată nesupravegheat și în locații cu risc mai ridicat de efracție sau delapidare un echipament de calcul utilizat în scop profesional, de serviciu;
- Utilizați în rețelele de date de serviciu numai echipamente de calcul pe care este instalat numai software cu licență validă (care nu sunt piratate), care nu au software malware instalat și care nu prezintă risc de securitate cibernetica;
- Păstrați credentialele (nume de utilizator, parole, coduri pin etc.) criptate, utilizând aplicații dedicate acestui scop și validate de către compartimentul IT al instituției dumneavoastră. Nu păstrați credențiale scrise pe foi de hârtie în loc vizibil, sau în format electronic în clar (necriptate).
- Solicitați compartimentului IT al instituției dumneavoastră o copie în format hârtie sau electronic a ghidului, sau manualului de utilizare a echipamentelor de calcul în interiorul, sau în interesul unei instituții publice;
- Instalați și utilizați numai programe și fișiere (inclusiv documente și fișiere multimedia) publicate sub licență validă (comercială, gratuită, sau deschisă) și care provin din surse sigure, legitime și verificabile;
- Pentru orice problemă de securitate identificată sau suspectată, deconectați echipamentul de calcul suspectat de la rețeaua de date și contactați de urgență compartimentul IT al instituției dumneavoastră;
- Dacă utilizați echipamente de calcul personale în scop profesional, aplicați toate regulile de mai sus și în ceea ce privește utilizarea și administrarea acestora.

2.1. Reguli privind utilizarea stațiilor de lucru

Pentru a asigura integritatea calculatorului și a datelor personale, vă recomandăm respectarea următoarelor reguli:

- Atunci când este posibil, încercaţi să utilizaţi sisteme de operare şi platforme hardware moderne. Multe dintre caracteristicile de securitate ale acestor sisteme sunt acum activate implicit şi pot preveni o multitudine de atacuri des întâlnite. Mai mult, versiunile acestor sisteme de operare pe 64 de biţi solicită eforturi mai mari din partea unui atacator care încearcă să capete controlul unui computer;
- O setare obligatorie, indiferent de sistemul de operare pe care îl folosiţi, este de a activa mecanismele automate de actualizare (update) ale sistemului de operare;
- Instalați o soluție de securitate ce oferă cel puțin protecție de tip antivirus, antimalware, antispam și antiphishing. O soluţie completă de securitate trebuie să ofere și capabilităţi de tip

firewall și IPS (Intrusion Prevention System), de prevenire a atacurilor şi de navigare securizată. Aceste servicii, utilizate împreună, pot oferi o apărare stratificată împotriva celor mai des întâlnite ameninţări. Multe dintre aceste soluţii oferă şi un serviciu care verifică site-urile pe care le accesaţi, având un istoric al reputaţiei domeniilor web care au avut vreodată un rol în răspândirea de malware;

- Nu uitaţi să activaţi orice serviciu de actualizare automată a acestor softuri de securitate pentru a vă asigura că folosiţi ultimele versiuni de semnături ale programelor antimalware;
- Evitaţi pe cât posibil folosirea contului de administrator al sistemului de operare. Este necesară crearea unui cont de utilizator care să nu aibă toate privilegiile specifice contului de administrator. Acest cont va fi folosit pentru activităţile uzuale, cum ar fi web-browsing, creare sau editare de documente, acces la e-mail etc. Contul de administrator ar trebui folosit numai atunci când se fac actualizări de software sau când este necesară reconfigurarea sistemului. Navigarea pe web sau accesul la e-mail folosind contul de administrator este riscantă, dând ocazia atacatorilor să preia controlul asupra sistemului;
- Folosiţi versiuni ale aplicaţiilor de tip Office cât mai recente. În versiunile mai recente, formatul de stocare al documentelor este XML, un format care nu permite executarea de cod la deschiderea unor documente, astfel protejând utilizatorii de malware-ul ce foloseşte ca mod de propagare astfel de documente. Unele din versiunile cele mai recente oferă o facilitate de tip “protected view”, deschizând documentele în modul “read-only”, astfel eliminând o serie de riscuri generate de un fişier infectat;
- Actualizaţi-vă software-ul! Majoritatea utilizatorilor nu au timpul sau răbdarea de a verifica dacă aplicaţiile instalate pe computer sunt actualizate. De vreme ce există multe aplicaţii ce nu au capabilităţi de auto-actualizare, atacatorii vizează astfel de aplicaţii ca mijloace de a prelua controlul asupra sistemului;
- Utilizați parole complexe. Ca o regulă generală, toate parolele asociate cu orice cont de utilizator ar trebui să aibă cel puţin 10 caractere şi să fie complexe, în sensul de a include caractere speciale, cifre, litere mici şi litere mari;
- Conturile de e-mail, atât cele web-based, cât şi cele locale, sunt ţinte foarte vizate de atacatori. Următoarele recomandări se pot dovedi utile pentru a reduce riscurile legate de acest serviciu:
    - În ideea de a nu vă compromite atât contul de e-mail de la birou, cât şi cel personal, este recomandat să folosiţi nume diferite pentru aceste conturi. Numele de utilizator unice pentru aceste conturi diminuează riscul de a fi vizate ambele conturi într-un atac;

- Setarea unor mesaje de genul “out-of-office” pentru contul personal de e-mail nu este recomandată, fiind o sursă preţioasă de informaţii pentru spammeri şi confirmând faptul că este o adresă de e-mail validă;
- Folosiţi întotdeauna protocoale securizate atunci când accesaţi e-mailul (IMAPS, POP3S, HTTPS), mai ales atunci când folosiţi o reţea wireless. Majoritatea clienţilor de email suportă aceste protocoale, prevenind astfel o interceptare a e-mailului atunci când este în tranzit între computerul dumneavoastră şi serverul de e-mail;
- E-mailurile nesolicitate, care conţin ataşamente sau link-uri, trebuie tratate ca suspecte. Dacă identitatea celui care a trimis respectivul e-mail nu poate fi verificată, sfatul este de a şterge acel e-mail fără a-l deschide pentru a-i vedea conţinutul. Nu răspundeţi la e-mailuri care vă solicită date cu caracter personal. Orice entitate cu care relaţionaţi prin intermediul unor aplicaţii web ar trebui deja să aibă aceste informaţii. În cazul e-mailurilor care conţin link-uri, nu navigaţi direct către acel link. Puteţi copia acel link şi să îl căutaţi de exemplu pe Google. Dacă este absolut necesară deschiderea unui atașament, se recomandă ca acesta să fie descărcat și scanat cu soluția antivirus instalată pe calculator;
- Nu vă lăsați amăgiți de probleme privind cardul de credit, sau invitații diverse care provin din partea unor surse necunoscute. Atunci când găsiți astfel de mesaje în Inbox, luați legătura cu banca (sau mergeți personal la bancă) pentru a vă asigura ca totul este în regulă referitor la contul dumneavoastră;
- Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin atașamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informații;
- Este greu de imaginat că o agenție guvernamentală v-ar contacta prin Internet pentru a colecta o amendă, așadar, tratați astfel de mesaje cu suspiciune, și sub nici o formă nu accesați link-urile sau atașamentele conținute de mesajul respectiv. În această situație, chiar și existența unei soluții de securitate eficiente, factorul uman joacă un rol decisiv. Ingineria socială poate ajuta un hacker sau un program să stabilească o conexiune cu utilizatorul, și convingerea acestuia în a oferi date critice sau bani. De asemenea, încercați să contactați un reprezentant al instituției, care să vă ofere cât mai multe informații posibil;

- Browserele sunt programele folosite pentru navigarea pe internet. Ele permit accesarea şi vizualizarea site-urilor, navigarea prin link-uri, descărcarea de fişiere de pe internet etc. Pentru a reduce riscurile legate de navigarea pe internet, ar trebui respectate următoarele recomandări:

- Utilizaţi browsere web cu capabilităţi de tip Sandbox. În momentul de faţă, există câteva astfel de browsere, care, atunci când se execută un cod malware, izolează acest cod de sistemul de operare, făcând astfel imposibilă exploatarea unei eventuale vulnerabilităţi a sistemului de operare. Majoritatea acestui gen de browsere au şi capabilitatea de auto-actualizare sau de notificare a utilizatorului atunci când apar versiuni noi;
- Evitați să accesați link-uri care sunt marcate drept periculoase de către soluția de securitate instalată pe sistem, sau de către browser-ul de internet. Dacă primiți orice mesaj de atenționare în timpul navigării pe o pagină, ieșiți imediat de pe respectiva pagină de internet;
- Atunci când este posibil, este recomandat să folosiţi versiunile criptate ale protocoalelor utilizate de aplicaţiile web. Criptarea la nivel de aplicaţie (numită SSL - Secure Soket Layer) asigură confidenţialitatea informaţiilor atunci când sunt în tranzit prin alte reţele. Marea majoritate a browsere-lor web indică faptul că o aplicaţie foloseşte SSL, folosind simbolul unui lacăt plasat lângă URL-ul respectivului site. Acest gen de criptare previne furtul de identitate de către eventuali atacatori care interceptează traficul din reţele wireless şi care ar putea să vadă credenţialele atunci când vă autentificaţi la aplicaţii web. Multe dintre aplicaţiile foarte populare precum Facebook sau Gmail sunt implicit configurate să folosească această criptare.;
- Atunci când doriți să efectuați cumpărați online, asigurați-vă că este un website pe care îl cunoașteți dinainte și, alternativ, verificați cât mai multe comentarii ale utilizatorilor despre serviciile respectivului website;
- Dezactivaţi executarea scripturilor în browsere. Dacă folosiţi anumite browsere, puteţi folosi opțiunea NoScript / NotScript sau plugin-uri pentru a nu permite execuţia de scripturi ce provin de pe site-uri necunoscute. Dezactivarea execuţiei de scripturi poate cauza probleme de folosire facilă a browserului, dar este o tehnică foarte eficientă pentru a elimina o serie de riscuri legate de execuţia acestor scripturi;

- Evitaţi schimbul de date între computerul de la locul de muncă şi cel de acasă. În general, reţelele companiilor sunt configurate de o manieră mai sigură şi au servicii (filtrare de e-mailuri, filtrare conținut web, IDS etc.) care pot detecta conţinutul maliţios. De vreme ce acasă, utilizatorii nu au aceleaşi reguli de securitate ca la locul de muncă, computerele personale sunt ţinte mult mai uşor de compromis pentru un atacator. Astfel, fluxul de date (folosind e-mailul sau stick-uri de memorie, etc.) dinspre computerul de acasă spre cel de la birou induce o serie de riscuri şi trebuie evitat de câte ori este posibil;

- Nu instalați software-ul dorit din locații despre care nu sunteți sigur, mai ales software care pare să fie de tip codec (program sau o bibliotecă de software, eventual chiar și un aparat hardware corespunzător, care asigură codarea și decodarea unei informații). În schimb, accesați pagina producătorului pentru a descărca acest tip de program.

2.2. Reguli privind utilizarea dispozitivelor mobile

2.2.1. Reguli privind utilizarea echipamentelor portabile de tip laptop

Regulile de utilizare a echipamentelor portabile de tip laptop sunt similare cu cele privind utilizarea stațiilor de lucru. Suplimentar, având în vedere caracterul mobil al acestor dispozitive, ar trebui respectate următoarele recomandări:

- Este recomandat să aveţi tot timpul controlul asupra laptop-urilor deoarece acestea pot fi ţinta unui atac dacă un atacator ar avea acces la ele. Dacă sunteţi nevoit să lăsaţi, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit şi să aibă discurile criptate. Sistemele de operare recente oferă nativ capabilitatea de criptare a discurilor prin mecanisme proprii. Pentru versiuni mai vechi, dar și pentru celelalte există produse care implementează acest serviciu. Astfel, puteţi evita accesul neautorizat la informaţii confidenţiale, în caz că laptop-ul este pierdut sau furat;
- În diverse locuri (cafenele, hoteluri, aeroporturi etc.) se găsesc hotspot-uri wireless sau chioşcuri care oferă servicii internet clienţilor. Având în vedere că infrastructura ce deserveşte aceste reţele este una necunoscută şi că adeseori, securitatea nu e o preocupare în aceste locuri, există o serie de riscuri. Pentru a le contracara, iată câteva recomandări:
    - Dispozitivele mobile ar trebui să fie conectate la internet folosind reţelele 3G/4G, această modalitate fiind de preferat în locul hotspot-urilor WiFi;
    - Dacă se foloseşte un hotspot Wi-Fi pentru accesul la internet, indiferent de reţeaua folosită, utilizatorii pot seta un tunel VPN către un furnizor de încredere pentru acest gen de servicii, protejând astfel tot traficul de date efectuat şi prevenind activităţi răuvoitoare cum ar fi interceptarea traficului;
    - Dezactivați funcția ”Network Share” înainte de a vă conecta la un hotspot public;
    - Utilizați o aplicație firewall care să filtreze accesul din exterior;
    - Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa internetul, este recomandat să vă rezumaţi doar la navigarea pe web şi să evitaţi să accesaţi servicii unde trebuie să vă autentificaţi, deci să furnizaţi date de genul user/parolă;
        - Evitați să faceți cumpărături online atunci când sunteți conectați la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri. De obicei,

informațiile schimbate între dumneavoastră și magazinul online, nu sunt criptate, și pot fi interceptate ușor de către un atacator. În orice caz, dispozitivele utilizate pentru serviciu nu ar trebui utilizate pentru activități personale;

- Nu folosiți niciodată calculatoare publice pentru a efectua tranzacții bancare, sau pentru alte tipuri de achiziții online. Aceste calculatoare ar putea conține programe care înregistrează datele personale, precum troienii bancari.

2.2.2. Reguli privind utilizarea echipamentelor portabile de tip tabletă şi smartphone

În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite și necesită o abordare specială. Principalele probleme care pot apărea, sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, fură informații sensibile și direcționează utilizatorii către site-uri și documente compromise. Următoarele reguli vor contribui la reducerea riscurilor:

- Actualizaţi-vă sistemele de operare pentru dispozitivele mobile. Este recomandat să faceţi acest lucru atunci când apar versiuni noi și să verificați acest lucru periodic. Sunteți mult mai vulnerabili atunci când utilizați dispozitivele mobile (telefon, tabletă etc.) în timpul unor călătorii, deoarece amenințările, sunt probabil mai prezente în rețelele publice din aeroporturi, gări, obiective turistice etc.
- Protejați-vă terminalul cu parole și opțiuni de criptare. În cazul în care cineva vă fură sau vă găsește telefonul/tableta, îngreunați-i accesul la informațiile stocate. De asemenea, criptați datele cu ajutorul unui software dedicat sau – dacă dispozitivul o permite – cu ajutorul opțiunii de criptare disponibilă în terminal;
- Folosiți o soluție de securitate care să aibă un modul antifurt, în mod special dacă folosiți un echipament care rulează Android. Din cauza cotei de piață ridicate, telefoanele/tabletele bazate pe Android au devenit ținta predilectă a infractorilor informatici. Alegeți însă o sursă reputată și urmăriți furnizorii care oferă și soluții de securitate pentru PC pentru a evita soluțiile de securitate false. O soluție antivirus vă permite să filtrați aplicațiile potențial periculoase și să le blocheze înainte ca acestea să cauzeze modificări asupra sistemului. În cazul în care pierdeți echipamentul sau vă este furat, modulul antifurt vă poate ajuta să identificați și să îl recuperați. De asemenea acesta poate fi utilizat pentru a bloca echipamentul sau pentru a şterge informaţiile de pe el de la distanţă. În cazul telefonului aceste operaţii pot fi efectuate chiar dacă acesta nu are acces la internet, un simplu SMS putând fi utilizat pentru blocarea acestuia sau pentru ștergerea informaţiilor personale;

- Sincronizați-vă telefonul/tableta cu un calculator personal. În cazul în care pierdeți aceste echipamente sau vă sunt furate, veți avea o copie de siguranță a contactelor, mesajelor, imaginilor și documentelor stocate pe acestea;
- Accesați doar hotspot-uri sigure. Asigurați-vă că opțiunile de conexiune prin infraroșu, Wi-Fi și Bluetooth-ul sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil;
- Fiți atenți ce aplicații descărcați și de unde. Să fie descărcate numai din magazinele oficiale ale operatorilor și producătorilor precum Google Play, Apple App Store sau Microsoft Store. Soft-urile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta și pot trimite mai departe, unor terțe părți informații private. În zone necunoscute, ați putea fi tentați să descărcați aplicații care să vă ajute să găsiți diferite locații precum restaurante, hoteluri sau muzee. Aveți însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea din greșeală a aplicațiilor nesigure, verificați configurația terminalului accesând SETĂRI, SECURITATE și asigurându-vă că opțiunea SURSE NECUNOSCUTE este nebifată.
- Fiți atenți la ofertele prea bune pentru a fi reale. Dacă primiți dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la prețuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignorați-le. Un click pe link-urile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completați formulare cu informații personale. Nu uitați de asemenea că telefonul/tableta dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website;
- Când folosiți rețelele sociale, asigurați-vă că fotografiile făcute cu smartphone-ul și pe care doriți să le încărcați pentru a le partaja cu prietenii, nu conțin informații legate de poziția dumneavoastră actuală. Partajarea locației e ideală pentru întâlnirile cu amicii în locuri publice, dar în același timp, permit persoanelor rău-intenționate să vă monitorizeze obiceiurile și rutina zilnică facilitând tentativele de hărțuire;
- Aveți mare grijă la ce fotografiați. Puteți fi tentat să fotografiați și să procesați coduri QR (coduri de bare care stochează informații despre diverse produse sau linkuri către website-uri). Dacă fotografierea și procesarea codurilor QR de pe ambalajele produselor nu sunt, de obicei, periculoase, puteți găsi coduri QR lipite în locuri publice sau chiar desenate pe elemente de mobilier stradal, ziduri etc. Aceste coduri pot conține URL-uri către website-uri care să exploateze vulnerabilități din telefonul dumneavoastră care să se finalizeze cu o infecție.

2.3. Reguli de folosire a propriilor dispozitive la locul de muncă

Majoritatea instituțiilor permit angajaților introducerea propriilor dispozitive mobile în sediu și folosirea acestora în desfășurarea activității. Pentru securitatea dumneavoastră și a rețelei instituției în care lucrați, vă sfătuim să urmați aceste reguli:

- Informați departamentul IT de faptul că aveți un dispozitiv personal pe care doriți să-l folosiți la serviciu. Echipa IT vă va introduce dispozitivul în rețeaua instituției și vă va informa asupra regulilor de utilizare și întreținere a echipamentului în interiorul instituției;
- Anunțați de urgență pierderea unui dispozitiv mobil pe care aveți date care aparțin instituției. Acest lucru este esențial pentru limitarea accesului unei persoane neautorizate la aceste informații. În cazul pierderii, echipa IT vă va arăta cum să vă ștergeți de la distanță conținutul telefonului;
- Nu uitați că un smartphone e și un dispozitiv de stocare portabil. Scanați conținutul memoriei interne și externe a telefonului la fiecare introducere în calculatorul de serviciu cât și în cel de acasă. In acest fel, nu veți transfera viruși de la serviciu, acasă și viceversa;
- Din același motiv, nu introduceți nici un dispozitiv de stocare găsit (de exemplu, USB stick, CD/DVD-ROM, card SD etc.) în calculatoarele instituției. Majoritatea atacurilor asupra rețelei instituțiilor încep cu un astfel de dispozitiv "uitat" de atacator în lift, în parcare sau în locuri din instituție în care e permis accesul personalului de întreținere sau a publicului (recepții, spații de aprovizionare etc.).

2.4. Reguli de prevenire a accesului neautorizat la informații confidențiale

Multe dintre atacurile cibernetice ce vizează furtul de date confidențiale din cadrul organizațiilor sunt realizate cu complicitatea unor persoane din interior, fie că vorbim de angajați sau persoane din exterior care au acces în spațiile unde sunt amplasate sistemele informatice (spre exemplu reprezentanții companiilor cu care organizația derulează diferite activități contractuale).

O altă tehnică din ce în ce mai utilizată de atacatori este ingineria socială, cunoscută ca „social engineering" în limba engleză, care presupune exploatarea vulnerabilităților psihologice ale oamenilor pentru a-i determina să întreprindă anumite acțiuni sau să divulge informații confidențiale fără să conștientizeze acest lucru. Un exemplu clasic este acela în care atacatorii sună un angajat al organizației țintă și încearcă obținerea de informații confidențiale (numele altor persoane din organizație, credențiale de acces la anumite sisteme informatice etc.) dându-se drept cineva din interiorul organizației (o persoană cu atribuții de conducere, un angajat de la alt departament sau reprezentantul unor furnizori etc.).

Pentru a evita accesul unor persoane neautorizate la informații confidențiale vă recomandăm următoarele:

- Evitați divulgarea de informații confidențiale la telefon sau prin email, daca nu puteți verifica identitatea celui cu care comunicați . Încercați să verificați identitatea persoanei care va cere aceste informații, o metodă eficientă fiind contactarea persoanei printr-un mijloc cunoscut (sunați pe nr. de telefon mobil al acestuia, contactați o persoană din apropierea acestuia etc.);
- Manifestați precauție la accesarea emailurilor. Nu deschideți mesajele email venite de la surse nesigure (expeditor necunoscut, subiect și conținut suspect) și a link-urilor sau atașamentelor conținute de acestea;
- Păstrați credențialele (nume utilizator, parolă, token etc.) de acces la sistemele informatice în siguranță. Evitați păstrarea acestora la vedere (pe monitor, tastatură, birou etc.);
- Închideți sesiunea de lucru (logoff) când părăsiți biroul unde se află computerul. Se recomandă setarea unui screensaver care să se activeze automat după un interval de maxim 2 minute de pauză în interacțiunea cu computerul;
- Manifestați precauție la introducerea credențialelor de acces la computer în prezența altor persoane pentru a nu fi observate de aceștia.

3. Ghid de îmbunătățire a securității unui computer

Pentru a asigura securitatea calculatorului trebuie urmate câteva principii, cum ar fi folosirea de firewall-uri, programe antivirus, filtre pentru e-mail şi parole. Principalele sfaturi pentru a asigura securitatea calculatorului sunt:

a) Actualizaţi în permanență sistemul de operare;
b) Instalaţi un program antivirus eficient;
c) Folosiţi un Firewall;
d) Securizaţi browser-ul dumneavoastră;
e) Descărcaţi programe numai din surse sigure/legitime;
f) Nu deschideţi ataşamentele suspecte ale e-mail-urilor;
g) Parolaţi conturile, schimbaţi parolele şi nu folosiţi aceeaşi parolă pentru toate conturile;
h) Realizați copii de siguranță (backup) pentru datele importante;
i) Raportați către structura IT, sau responsabililor cu securitatea informatică a sistemelor informatice din organizație, orice comportament suspect al stațiilor de lucru, cum ar fi, apariția excesivă a ferestrelor de tip pop-up, performanța extrem de slabă a computer-ului sau un browser de Internet extrem de lent.

Trebuie menţionat că în unele instituţii există o persoană specializată în administrarea calculatoarelor şi a reţelelor (numit de obicei *administrator de sistem* sau *IT manager*). Printre atribuţiile acestuia se

numără în cele mai multe cazuri şi asigurarea securităţii calculatoarelor, iar uneori şi aspectele legate de arhivare şi back-up. Dacă aveţi o problemă legată de securitate, este indicat să apelaţi mai întâi la un astfel de specialist pentru a o soluţiona.

Este recomandat ca în orice instituţie să existe un astfel de administrator de sistem sau o firmă externă, care să îndeplinească rolul acestuia atunci când e nevoie. În cazul în care nu puteţi apela la un administrator de sistem, este indicat să urmaţi sfaturile detaliate mai jos, pentru a vă proteja calculatorul:

Actualizaţi în permanenţă sistemul de operare

Actualizarea sistemului de operare reprezintă alegerea şi instalarea celor mai recente componente, perfecţionări, îmbunătăţiri, actualizări de securitate şi drivere pentru computer. Această actualizare trebuie să se realizeze cât mai des, astfel încât calculatorul să ruleze optim şi să fie cât mai puţin vulnerabil la atacuri sau viruşi.

Majoritatea programelor şi a sistemelor de operare pot fi actualizate vizitând pagina de web a acestora şi instalând cele mai noi componente, module etc. Sistemele de operare moderne oferă un program integrat în sistem, care atenţionează automat utilizatorul despre apariţia acestor componente noi şi facilitează instalarea lor (Actualizări Automate – Automatic Updates).

Instalaţi pe calculatorul dumneavoastră un program antivirus eficient

Programele antivirus identifică viruşii cu ajutorul unei baze de date, şi dacă pe parcursul scanării întâlneşte un fişier modificat de un virus, atenţionează utilizatorul, oferind posibilitatea de ştergere sau "corectare" a fişierelor afectate. Întrucât corectarea nu este întotdeauna posibilă (caz în care se pot pierde date importante), cel mai eficient mijloc de a vă feri calculatorul de acţiunea viruşilor este împiedicarea instalării acestora.

Pentru aceasta, ţineţi seama de următoarele recomandări:

- Scanaţi cu un program antivirus actualizat orice suport (dischetă, stick USB, CD, DVD) pe care îl introduceţi în calculator şi abia pe urmă folosiţi datele stocate pe acestea;
- Scanaţi toate fişierele descărcate de pe Internet şi cele primite ca ataşament prin e-mail înainte de a le deschide sau salva în calculator;
- Păstraţi programul antivirus în funcţiune pe toată perioada sesiunii de lucru la calculator, pentru ca acesta să monitorizeze automat fişierele în uz;
- Actualizaţi în mod regulat programului antivirus astfel încât acesta să cuprindă definiţiile viruşilor nou apăruţi şi mijloacele de combatere a acestora. În prezent majoritatea programelor antivirus se actualizează on-line în mod automat.

Folosiţi un program Firewall

Programele firewall sunt folosite pentru a proteja calculatorul de pătrunderi neautorizate şi de viruşi. Firewall-ul filtrează toate informaţiile care vin şi pleacă spre/dinspre calculator, în funcţie de anumite criterii prestabilite (destinatar/expeditor, tipul informaţiei etc.).

Firewall-ul poate împiedica persoanele străine (de ex. hackerii, dar şi programele create de aceştia, cum ar fi viermii şi anumite tipuri de viruşi) să intre pe computerul dumneavoastră prin Internet. Utilizarea unui firewall este importantă în special dacă sunteţi conectat în permanenţă la Internet (de exemplu când aveţi o conexiune prin cablu sau prin linii DSL sau ADSL).

Un firewall poate lua două forme, software sau hardware. Cele hardware sunt mai rar întâlnite şi sunt în general instalate şi întreţinute de administratorul de reţea. Pentru a instala un firewall software, se pot folosi programe gratuite (disponibile pe Internet) sau achiziţionate, unele fiind chiar incluse în sisteme de operare mai recente.

Controlaţi ceea ce rulează în browser-ul dumneavoastră

Când browser-ul descarcă un program pe calculatorul dumneavoastră, va căuta informaţii despre programul respectiv şi despre firma care l-a creat. În cazul în care aceste informaţii sunt găsite, veţi fi întrebat dacă doriţi să instalaţi programul în cauză. Dacă informaţiile despre program nu sunt disponibile, instalarea obiectului este riscantă şi browser-ul vă va avertiza în acest sens.

Securitatea navigării în Internet poate fi crescută prin stabilirea nivelului de securitate a browserului, acesta putând bloca anumite programe sau putând cere confirmări pentru a permite rularea lor.

Descărcaţi programe numai din surse sigure

Este bine să limitaţi descărcarea şi instalarea de programe de pe Internet la strictul necesar şi acest lucru să se facă din site-uri sigure. Evitaţi să descărcaţi fişiere din grupurile de discuţii publice, deoarece accesul la acestea este nelimitat şi riscul este pe măsură!

De asemenea, evitaţi să deschideţi sau să descărcaţi ataşamente suspecte primite prin e-mail, mai ales dacă provin din surse necunoscute. Obişnuiţi-vă să verificaţi cu un program antivirus absolut tot ce intră în calculator – de la dischete, stick-uri USB şi CD-uri, până la e-mail-uri şi ataşamentele acestora. Este întotdeauna mai indicat să previi decât să remediezi.

Nu deschideţi ataşamentele suspecte ale e-mail-urilor

Aşa cum s-a arătat mai sus, cea mai frecventă metodă de răspândire a aplicaţiilor maliţioase este prin e-mail. Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text sau printr-un titlu interesant al ataşamentului, însă ataşamentul lansează în fapt un virus sau o altă aplicaţie maliţioasă.

Ca atare, este indicat să nu deschideţi ataşamentele despre care nu sunteţi convinşi că sunt documente utile.

Parolaţi conturile, schimbaţi parolele şi nu folosiţi aceeaşi parolă pentru toate conturile

Pentru a evita accesul unor persoane străine la calculatorul dumneavoastră, la diversele aplicaţii cu informaţii confidenţiale sau la conturile de e-mail, este indicat să folosiţi parole de acces pe care să le cunoaşteţi numai dumneavoastră. Este indicat să folosiţi parole diferite pentru diferitele conturi, astfel ca, în eventualitatea că o persoană străină descoperă parola pentru un anumit cont, aceasta să nu obţină automat acces la toate conturile dumneavoastră.

Câteva reguli de urmat la stabilirea de parole:

- nu folosiţi:
    - numele dumneavoastră, al altcuiva din familie sau al animalului preferat,
    - elemente ale adresei dumneavoastră: numele clădirii, străzii, ţării,
    - denumirea instituției, a proiectului etc.,
    - numărul de telefon, numărul de înmatriculare
    - numele starului sau personajului preferat (sau al filmului, cărţii etc.),
    - cuvinte din dicţionar;
    - numele contului pentru care stabiliţi parola;
- utilizaţi combinaţii de caractere mici şi majuscule, cifre şi alte caractere (de ex. #, &, %, $, @);
- utilizaţi parole mai lungi de 6 caractere;
- schimbaţi parola de cel puțin două ori pe an.

Exemple de parole:

- parola bună - %C26p03A1979$
- parole de evitat – 123456, qwerty, parola, hacker, primarie etc.

Faceţi Back-up pentru datele importante

Întrucât există numeroşi factori de risc şi datele stocate pe calculator sunt adesea mai valoroase decât însuşi calculatorul, aceste date trebuie arhivate periodic – operaţie numită „back-up”. Această operaţiune trebuie realizată frecvent (în funcţie de importanţa informaţiilor, arhivarea se poate face lunar, săptămânal sau zilnic – în unele cazuri chiar mai des), deoarece datele pierdute sunt adesea imposibil de recuperat.

4. Indicii de infectare a computerului

Utilizatorii sunt adesea sfătuiți să verifice periodic sistemul împotriva infectărilor, însă în condițiile scenariilor actuale ale atacurilor informatice, acest lucru nu mai este de ajuns. Frecvent, este nevoie de mai mult decât de informații de bază despre securitate IT, pentru a remedia un calculator infectat, iar mulți utilizatori începători nu au cunoștințe despre acest lucru. În condițiile în care multe amenințări din prezent sunt create special pentru a nu fi detectate, există totuși câteva indicii prin care putem identifica un calculator compromis.

Cele mai răspândite 10 semne de infectare sunt:

1. “Computerul vorbește cu mine“. Apar pe ecran tot felul de ferestre “pop-up” și mesaje publicitare, precizând că PC-ul este infectat și că are nevoie de protecție. Acesta este un exemplu tipic de infectare. Este vorba fie de un program spion (“spyware”) în computer sau de o infectare cu un antivirus fals (numit și “rogueware“);
2. “Computerul meu funcționează extrem de încet“. Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. În cazul în care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, făcându-l să funcționeze mai greu decât de obicei;
3. “Aplicații care nu pornesc”. De câte ori ați încercat să porniți o aplicație din meniul start sau de pe desktop și nimic nu se întâmplă? Uneori se poate deschide chiar un alt program. Ca și în cazul anterior, poate fi vorba de orice altă problemă, însă este cel puțin un simptom care vă spune că ceva nu este în regulă;
4. “Nu mă pot conecta la Internet sau acesta rulează extrem de încet“. Pierderea accesului la Internet este un alt semn al infectării, deși poate fi cauzat și de probleme legate de furnizorul de Internet sau router. Pe de altă parte, este posibil să aveți o conexiune la Internet care funcționează mult mai greu decât de obicei. Dacă ați fost infectat, malware-ul se poate conecta la o anumită adresă de Internet sau poate deschide anumite conexiuni separate, limitând astfel viteza de accesare a Internetului sau chiar făcând imposibilă folosirea acestuia;
5. “Când mă conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate”. Acesta este cu siguranță un alt semn al infectării cu malware. Multe fișiere virale sunt concepute special pentru redirectarea traficului de Internet către anumite website-uri, fără consimțământul utilizatorului, sau chiar să imite anumite website-uri, creând impresia unui site legitim;
6. “Unde au dispărut fișierele mele?“ . Să sperăm că nimeni nu va pune această întrebare, deși anumite atacuri sunt concepute special pentru criptarea sau ștergerea anumitor fișiere și chiar

mutarea documentelor dintr-un loc în altul. Dacă vă găsiți în această situație, este cazul să începeți să vă faceți griji;

7. “Antivirusul meu a dispărut, firewall-ul este dezactivat”. O altă acțiune tipică a amenințărilor de pe Internet este dezactivarea sistemelor de securitate (antivirus, firewall etc.) instalate pe calculator. Dacă un singur program s-ar opri, poate că ar fi vorba de o eroare de software, dar dacă toate componentele de securitate s-ar dezactiva, aveți cu siguranță computerul infectat;
8. “Computerul meu vorbește în altă limbă”. Dacă limba anumitor aplicații se schimbă, ecranul apare inversat, “insecte” ciudate încep să “mănânce” ecranul, este posibil să aveți de asemenea, un sistem infectat;
9. “Îmi lipsesc fișiere necesare pentru a rula jocuri, programe etc.”. Din nou, acest lucru ar putea fi un semn de infectare, deși este posibil să fie vorba de o instalare incompletă sau incorectă a acelor programe;
10. “Computerul meu practic nu mai poate fi controlat”. În cazul în care computerul dumneavoastră începe să acționeze singur sau să trimită email-uri fără să știți, dacă aplicații sau ferestre de Internet se deschid singure, în mod sporadic, sistemul ar putea fi compromis de malware.

5. Ameninţări cibernetice – breviar

5.1. Ransomware

Ransomware este un software malițios ce împiedică accesul la fișiere, sau chiar la întregul sistem infectat, până la plata unei „recompense”. Acest tip de malware nu reprezintă o noutate, însă pentru a îngreuna procesul de recuperare a fișierelor, ransomware-urile actuale blochează accesul la documente, fotografii, muzică, filme etc., prin criptarea asimetrică a acestora.

În continuare sunt prezentate câteva variante cunoscute de ransomware împreună cu indicații referitoare la prevenirea infecției cu acest tip de malware, dar și măsuri ce pot fi aplicate pentru limitarea impactului în cazul în care s-a produc infecția.

Recomandarea CERT-RO este să evitați plătirea recompensei solicitate, pentru că astfel contribuiți în mod direct la încurajarea acestui tip de activități frauduloase și riscați să nu re-dobândiți accesul la fișierele criptate nici după efectuarea plății.

5.1.1. CTB Locker

CTB Locker (*Curve-Tor-Bitcoin Locker*), cunoscut şi sub numele de **Critroni**, reprezintă un software maliţios de tipul *ransomware* al cărui scop este de a cripta fişierele stocate pe sistemul afectat. Acesta

a fost lansat la mijlocul lunii iulie a anului 2014 şi vizează toate versiunile de Windows, inclusiv Windows XP, Windows Vista, Windows 7, Windows 8 și Windows 10.

Odată infectat cu acest malware, sistemul afectat va fi scanat, iar fişierele regăsite pe acesta vor fi criptate. Este important de ştiut că, dacă în trecut fişierele criptate îşi schimbau extensia în **CTB** sau **CTB2**, ultimele versiuni de *CTB Locker* identificate adaugă fişierelor criptate o extensie aleatoare (spre exemplu **.ftelhdd**, **.ztswgmc**, etc.). După criptarea fişierelor, este deschisă o fereastră de răscumpărarea datelor precum cea din **Figura 1** de mai jos.

Pentru mai multe informații referitoare la această amenințare vă recomandăm parcurgerea articolului dedicat CTB Locker pe portalul CERT-RO:

https://www.cert.ro/articol.php?idarticol=905

Figura 1. Mesaj afișat utilizatorilor în urma infecției cu CTB Locker

5.1.2. CryptoWall

Ca și în cazul CTB Locker, și acest ransomware criptează fişierele stocate pe sistemul infectat şi apoi solicită o sumă de bani (500$, 500 EUR, 0.5 Bitcoin etc.) în schimbul decriptării acestora. CryptoWall 3.0/4.0 utilizează reţeaua *TOR* pentru direcţionarea utilizatorului victimă către pagina web unde acesta va regăsi instrucţiunile pentru modul de plată a „recompensei" şi decriptarea datelor. De asemenea atacatori au extins perioada de răscumpărare de la 5 zile la o săptămână, după care preţul pentru decriptarea fişierelor se va dubla.

Odată instalat pe sistemul infectat, *CryptoWall* începe procesul de criptare a fişierelor în fundal, fapt pentru care majoritatea utilizatorilor nu observă că sistemul lor a fost infectat până în momentul în care programul maliţios afişează fereastra de răscumpărare a fişierelor deja criptate.

CryptoWall 3.0 utilizează algoritmul de criptare *RSA-2048* pentru criptarea fişierelor. Odată finalizat procesul de criptare a fişierelor, malware-ul le şterge pe cele originale, iar în cazul în care nu există *backup* pentru acestea, şansele de a le recupera scad dramatic.

Scopul programului maliţios este de a cripta fişierele valoroase pentru utilizator. Acesta criptează pe lângă documentele MS Office, imagini, fişiere audio, video etc. Astfel de malware este de obicei greu de detectat de utilizatori deoarece se ascunde în spatele unui software legitim răspândit via email, site-uri web, drive-in downloads etc.

Mesajul de răscumpărare este un fişier HTML şi arată precum în figura de mai jos:

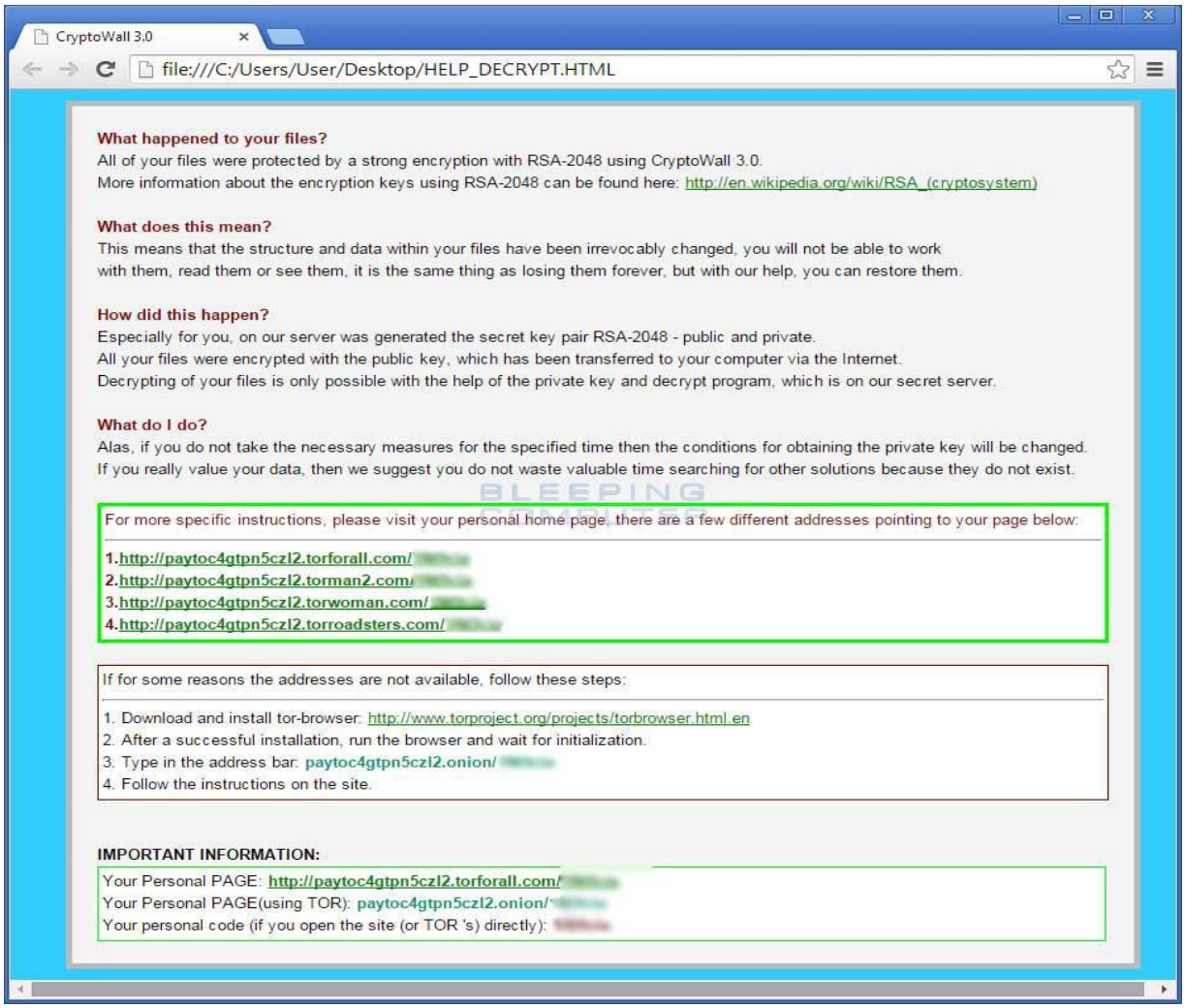

Figura 2. Mesaj afişat utilizatorilor în urma infecției cu CryptoWall

Pentru mai multe informații referitoare la această amenințare vă recomandăm parcurgerea articolului dedicat CTB Locker pe portalul CERT-RO:

https://www.cert.ro/articol.php?idarticol=931

5.2. Spyware

Programele de tip spyware sunt scrise cu scopuri malițioase. Ele se pot afișa extrem de simplu, ca niște ferestre de tip pop-up extrem de enervante, care au menirea să îți distragă atenția sau să te atragă către site-uri malițioase. Totodată, pot fi software-uri care înregistrează obiceiurile din browser-ul pe care îl folosești pentru navigarea pe Internet sau chiar intrările de la tastatură (keylogger), cu intenția de a capta credențiale de acces sau parole.

Utilizatorii sunt sfătuiți să raporteze cazurile de activitate suspicioasă pe stațiile de lucru, cum ar fi, apariția excesivă a ferestrelor de tip pop-up, performanța extrem de slabă a computer-ului sau un browser de Internet extrem de lent, care ar putea fi redirectat către site-uri nelegitime sau nedorite, precum cele pornografice sau cele de pariuri online. În astfel de cazuri trebuie să vă adresați pentru asistență Departamentului IT, și să raportați suspiciunea că stația dvs. a fost infectată cu spyware.

Cum vă protejați de spyware

Încercați să evitați accesarea site-urilor necunoscute și să le frecventați pe cele de încredere. Site-urile de încredere sunt de regulă foarte atent monitorizate de către administratorii acestora și foarte rar veți găsi software de tip spyware încorporat în astfel de pagini.

Recomandăm activarea caracteristicilor de securitate ale browser-ului folosit la navigarea pe Internet. Browsere precum Internet Explorer, Mozilla, Google Chrome sau Safari au astfel de setări incluse. Mai mult, vă recomandăm să dezactivați în browser stocarea fișierelor de tip *cookie* deoarece acestea pot fi folosite cu intenții malițioase. Descărcați programe și software numai de pe site-uri de încredere. Niciodată nu accesați ferestre pop-up nedorite. În schimb, închideți-le cu click pe butonul X care apare cu culoarea roșie de regulă în partea dreaptă sus a ferestrei pop-up.

Instalați software anti-spyware și actualizați-l periodic, la fel cum procedați și cu software-ul antivirus. Rulați acest software în mod regulat. Programe precum *SpyBot* și *AdAware* sunt gratuite și fac o treabă excelentă în ceea ce privește protejarea sistemului de spyware. În același timp, instalați un pop-up blocker de tip *AdBlock*.

Sfaturi pentru utilizarea în condiții de siguranță a Internetului, prevenind pătrunderea spyware-ului în rețeaua sau sistemul instituției

1. Nu descărcați niciodată deliberat, software de pe Internet pe stația de lucru, indiferent cât de productiv sau interesant pare. Chiar și inofensivele bare de instrumente sau utilități pot conține spyware. Atenție sporită la programe de tip file-sharing, pe care oricum nu ar trebui să le utilizați la birou;
2. Stați departe de orice site-uri dubioase, inclusiv pornografie, jocuri de noroc, hacking sau alte site-uri suspicioase/ne-convenționale. În orice caz, nu ar trebui să vizitați astfel de site-uri în desfășurarea atribuțiilor de serviciu;
3. Oricând apare o fereastră pop-up nedorită sau neașteptată, închideți-o imediat apăsând pe semnul X din partea dreapta sus a ferestrei. Niciodată nu dați click pe orice buton afișat, chiar dacă afișează mesajul "CANCEL" sau "CLOSE" pe fereastra în sine. Aceste butoane pot avea în spate o comandă pentru descărcare nedorită de spyware;
4. Fiți suspicioși în momentul în care numeroase ferestre pop-up încep să se afișeze pe ecranul computer-ului, sau dacă performanța sistemului este sesizabil afectată. Din acel moment puteți presupune că ați fost infectat cu spyware și va trebui să vă adresați departamentului IT;
5. Dacă folosiți Internet Explorer ca browser, schimbați setările pentru a bloca Active X. Mergeți la TOOLS > Internet Options > Security > Custom Level. În această fereastră există o secțiune în partea de sus, dedicată controalelor Active X. Aici vă sfătuim să dezactivați descărcarea de Active X cu sau fără semnătură, precum și cele marcate ca ''unsafe''. Unele obiecte Active X sunt spyware. Aceste setări le vor bloca.

5.3. Farse pe e-mail, Scam și Spam

Multe din incidentele de tip **Scam** vin sub forma unui avertisment despre un virus care poate să 'șteargă hard disk-ul' sau un mesaj similar. Mesajul îți va cere să contactezi toate persoanele din agenda dvs. pentru a-i avertiza. Aceste farse sunt extrem de comune, astfel că furnizorii de software antivirus au creat pagini web care raportează și urmăresc ultimele astfel de încercări.

Una dintre escrocheriile cele mai cunoscute și propagate via e-mail (SCAM) este cea care folosește mesajul 'You can be a millionaire' (Poți deveni milionar). Prin retransmiterea acestor e-mail-uri altor persoane, utilizatorul este convins că va primi o anumită sumă de bani pentru fiecare mesaj transmis. Au existat foarte multe persoane care au căzut pradă acestei scheme. Autorii acestui tip de e-mail caută adesea notorietate prin transmiterea mesajului lor, la cât mai mulți utilizatori.

O modalitate simplă de a sesiza o farsă sau înșelătorie este includerea unui atașament. La fel cum site-uri de încredere nu vor cere informații cu caracter personal prin e-mail, persoane de încredere sau instituții nu vă vor transmite printr-un atașament care trebuie folosit 'pentru eliminarea fișierelor

infectate. **Așadar, este foarte important să nu deschideți niciodată un atașament de la un expeditor necunoscut sau un atașament pe care nu îl așteptați.**

Țineți minte: În cazul în care mesajul sună prea frumos pentru a fi adevărat, atunci probabil că așa este. În cazul în care în corpul e-mail-ului se specifică faptul că urmărește numărul destinatarilor mesajului pe care ar trebui să îl transmiți mai departe, atunci este vorba de o înșelătorie. E-mail-urile nu pot fi urmărite în acest mod. Cel mai bun mod de a opri acest tip de farse și escrocherii, este de a te informa despre modul cum acestea operează. Informarea este cheia succesului în cazul eliminării campaniilor dăunătoare de pe Internet.

Spam-ul este adesea un efect secundar comun și adesea frustrant de a avea un cont de e-mail. Cu toate că nu vei putea niciodată elimina complet primirea unor astfel de mesaje, există totuși modalități de a reduce cantitatea de mesaje de tip spam primită.

Spam-ul este varianta electronică a *junk mail*-ului, termen referitor la mesaje nesolicitate și adesea nedorite de către destinatar. Tendința este ca și spam-ul să conțină un atașament sau link malițios.

Există câțiva pași pe care puteți să-i faceți pentru a reduce semnificativ cantitatea de spam pe care o primiți:

- Nu oferiți adresa de e-mail în mod arbitrar – adresele de e-mail au devenit așa de comune, încât au alocat un spațiu special pe aproape orice formular. Pare inofensiv, astfel că o mulțime de oameni completează adresa lor de e-mail în spațiul alocat de pe orice formular practic fără să realizeze ce se poate întâmpla cu aceasta. Spre exemplu, companiile de regulă introduc astfel de adrese de e-mail într-o bază de date pentru a putea ține evidența clienților și a datelor de contact aferente acestora. Uneori aceste liste sunt vândute sau partajate cu alte companii, astfel că din acel moment este posibil să primiți mesaje nesolicitate;
- Verificați politicile de confidențialitate – Înainte de a trimite o adresă de e-mail online, uitați-vă după o politică de confidențialitate. Cele mai renumite site-uri au încorporat un link către politica de confidențialitate pentru orice formular pe care vi se cere să îl completați cu date personale. Ar trebui să citiți atent această politică de confidențialitate înainte de a completa o adresă de e-mail sau orice alte informații personale;
- Raportați mesajele ca spam – Majoritatea clienților de e-mail (Thunderbird, Outlook etc.) oferă o opțiune de a raporta un mesaj ca spam sau junk. Dacă aveți această opțiune puteți profita de funcționalitatea ei. Raportând mesajele de tip spam sau junk folosind această funcționalitate, ajută la filtrarea corectă a mesajelor astfel încât e-mail-urile nedorite să nu mai fie afișate în Inbox. Cu toate acestea, instrumentele care fac această filtrare fiind automatizate, este de

dorit să verificați frecvent directoarele de tip SPAM sau JUNK pentru eventualitatea în care mesaje legitime pot ajunge la rândul lor în acest spațiu;

- Nu urmăriți link-urile din mesajele de tip spam – Unele mesaje spam se bazează pe generatoare care încearcă diferite variații de adrese de mail pe anumite domenii. Mesajele nedorite care oferă o opțiune de dezabonare sunt deosebit de tentante, dar acest lucru este de multe ori o metodă de colectare a adreselor valide care sunt apoi folosite pentru a trimite alte mesaje de tip spam;
- Dezactivați descărcarea automată a graficii în e-mail-uri HTML – Mulți dintre cei care trimit mesaje de tip SPAM trimit mesaje HTML cu un fișier grafic atașat, iar acesta este utilizat pentru a urmări cine deschide mesajul. În cazul în care clientul de mail descarcă graficul de pe serverul de web, expeditorul știe că mesajul a fost deschis. Dezactivarea afișării HTML cu totul și vizualizarea mesajelor în text simplu previne această problemă;
- Pentru spațiul personal, recomandăm deschiderea adițională a unui alt cont de e-mail, majoritatea furnizorilor importanți (Google, Microsoft, Yahoo etc.) oferind conturi de e-mail gratis. Dacă o anumită adresă de e-mail este foarte des utilizată (pentru cumpărături online, pentru autentificarea pe anumite servicii, etc.), o adresă secundară de e-mail ar putea fi folosită pentru protejarea celuilalt cont utilizat. Totodată, ați putea utiliza acest al doilea cont atunci când postați pe liste de discuții publice, pe site-uri de social networking, bloguri, forumuri sau web. În cazul în care contul începe să se umple cu spam vă recomandăm să ștergeți absolut toate mesajele și să vă notificați contactele despre noua adresă de e-mail pe care ați creat-o;
- Utilizaţi câmpul ”BCC:” pentru a trimite e-mail-uri. Câmpul "Bcc:" ajută la protejarea caracterului confidenţial al adreselor altor destinatari şi să conferim mesajului nostru un caracter unic şi special;
- Nu folosiţi adresa de e-mail primită de la serviciu în interes personal. De exemplu înscrierea pe diferite forumuri, rețele de socializare sau alte site-uri, precum şi recepționarea și/sau redistribuirea de mesaje de genul filmulețe comice, bancuri, fotografii sunt activităţi pentru care ar trebui utilizat un cont de e-mail personal.

5.4. Phishing

Phishing-ul este o metodă online folosită de către atacatori pentru a sustrage bani, credențiale de acces la conturi online, parole sau alte informații personale și/sau importante. De obicei, un atac de tip *phishing* reprezintă un e-mail deghizat ca un mesaj de la o sursă de încredere (bancă, companii de credit, comercianți online etc.). Nu este un fapt neobișnuit ca funcționarii publici să primească e-mail-uri de tip phishing care par să vină din partea colegilor de birou sau din partea altor angajați din

spațiul public. Aceste conturi au fost de cele mai multe ori compromise în prealabil și ulterior făcute să trimită e-mailuri de tip phishing către toate contactele înregistrate în lista lui de contacte.

Mesajul primit vă cere de regulă să verificați imediat datele contului dvs., amenințând de regulă cu luarea unor măsuri negative împotriva dvs. în cazul în care nu vă conformați. Utilizatorii sunt astfel adesea păcăliți în a furniza informațiile cerute cu caracter personal sau confidențial, cum ar fi numere de cont bancar sau de card de credit, codul numeric personal, parole, etc. Astfel de e-mail-uri pot conține imagini, logo-uri texte și link-uri către site-uri web ce par a fi legitime. De asemenea, este comun pentru astfel de e-mail-uri să includă atașamente și link-uri pentru documente false, care vă solicită să introduceți numele de utilizator și parola. Este foarte importantă verificarea legitimității oricăror atașamente venite din partea colegilor de muncă, angajați din spațiul public, sau din alte surse, înainte de a deschide documentul sau de a accesa link-ul transmis.

E-mail-urile legitime venite din partea instituțiilor financiare, angajați din domeniul public sau orice alt tip de organizație, nu îți vor solicita NICIODATĂ informații personale.

Cum puteți sesiza diferența dintre o înșelătorie de tip phishing și un e-mail sau site legitim?

Din nefericire, incidentele de tip phishing sunt din ce în ce mai răspândite și utilizate, dezvoltându-se și fiind din ce în ce mai greu de identificat. Cu toate acestea, există multiple strategii pe care le puteți utiliza pentru a recunoaște acest tip de escrocherii.

- Fiți sceptic! Din moment ce realizați faptul că astfel de escrocherii de tip phishing există în lumea virtuală, fiți sceptici cu privire la conținutul fiecărui email pe care îl primiți. A fost oare contul dvs. cu adevărat compromis? Aveți cu adevărat nevoie să vă actualizați informațiile contului? Majoritatea companiilor nu așteaptă până în ultimul moment să-și notifice clienții despre o situație de urgență. Aceștia de regulă trimit mai multe notificări, de regulă prin intermediul serviciului poștal sau vă contactează prin telefon pentru a vă avertiza asupra potențialelor încălcări ale securității. Dacă primiți astfel de email-uri, verificați conținutul pentru indicii care să demonstreze că acel mesaj este un fals;
- Verificați atent adresa web și adresa de email deopotrivă. Este o modalitate foarte bună de a descoperi o înșelătorie. Spre exemplu, în cazul în care o adresă web este afișată sub această formă (http://172.168.15.100/ebay/account/), atunci fiti sigur că site-ul pe care urma să îl accesați nu este unul legitim. Chiar dacă Ebay este parte a adresei afișate, după cum puteți observa, prima parte conține caractere numerice aranjate sub forma unei adrese IP. Acesta este un indiciu clar că ceva nu este în regulă;
- Uitați-vă după semne clare de securitate. Site-urile corporațiilor, de regulă sunt atent securizate și folosesc pagini web criptate de fiecare dată când clienților li se cere să trimită

informații cu caracter personal. În bara de navigare a browserului utilizat, verificați dacă adresa pe care doriți să o accesați începe cu 'https://'. Litera 's' reprezintă unul din semnele că această conexiune este securizată și vine din engleză de la termenul de 'security/secure'. Totodată, uitați-vă după o pictogramă cu un lacăt închis în partea de sus a ferestrei browserului. Dacă nu identificați aceste semne, atunci este posibil ca site-ul să fie unul fals;

- Atenție la detaliile dubioase! Majoritatea email-urilor sau website-urilor venite din partea corporațiilor au un aspect profesional. Phishing-urile încearcă să te păcălească, copiind aspectul acestora. Pentru a detecta diferențele, căutați în text greșeli gramaticale, de ortografie sau chiar greșeli de design cu privire la aspectul site-ului. Dacă instinctul îți transmite că e ceva dubios, atunci cel mai probabil ai dreptate. După cum am mai afirmat, escrocheriile de tip phishing devin din ce în ce mai complexe pe zi ce trece, astfel că parcurgerea pașilor propuși nu este o modalitate 100% sigură de detectare a unui phishing, dar este un punct de început;
- Folosiți telefonul pentru a vă asigura de legitimitatea conținutului. Sunați compania expeditoare a mesajului sau persoana în cauză, dar nu folosiți numărul de telefon afișat în corpul e-mail-ului. Contactați o persoană care ar putea cu adevărat să vă ajute să verificați legitimitatea mesajului primit.

Dacă simțiți că ați fi putut primi un e-mail de tip phishing, nu faceți click pe orice link-uri pentru a deschide atașamentele și nu transmiteți e-mailul mai departe.

5.5. Spear-phishing

Acest tip de phishing este o formă mai concentrată și vizează un anumit membru al unei instituții, care solicită accesul neautorizat la date confidențiale. Ca și în cazul mesajelor folosite în cazul campaniilor de tip phishing normale, mesajele de spear-phishing par că sunt expediate de la o sursă cunoscută și de încredere. În cazul spear-phishing-ului însă, sursa aparentă a e-mailului este cel mai probabil un individ din interiorul instituției recipientului sau dintr-o rețea de contacte de încredere, de regulă aflați într-o poziție de autoritate.

Conform NY Times, încercările de spear-phishing nu sunt de regulă inițiate de către atacatori în mod aleatoriu, dar sunt mai degrabă conduse de "grupuri sofisticate ce caută câștiguri materiale, secrete comerciale sau informații militare".

6. Definiții și termeni

Administratorul sistemului informatic şi de comunicaţii – este o persoană investită cu responsabilitate privind crearea, modificarea, dezvoltarea şi administrarea sistemelor informatice.

***Abuz de* privilegii** – reprezintă orice acţiune întreprinsă în mod voit de un utilizator, contrar prevederilor regulamentelor, politicilor, procedurilor şi legilor în vigoare.

Confidenţialitate – principiul securităţii informaţiei, conform căruia informaţia este accesibilă doar persoanelor autorizate în acest sens.

Informații confidențiale – acele informații generate, gestionate sau procesate în cadrul unei instituții, care nu pot fi furnizate către terți în formă brută (fără a fi prelucrate sau completate) sau care sunt marcate în consecință, în baza unor reglementări.

Disponibilitate – principiul securităţii informației, conform căruia utilizatorii au acces la informaţie atunci când au nevoie.

Echipament – În sensul prezentului ghid, prin echipament se înțelege un calculator, hub, switch, antenă, modem, router, server, telefon, tabletă sau orice alt dispozitiv informatic.

Eveniment de securitate – orice fapt sau situație relevantă din punct de vedere al securității cibernetice, ce poate produce o schimbare a stării de normalitate în cadrul unui sistem informatic, poate indica o posibilă încălcare a politicii de securitate sau o deficiența a acesteia, sau inclusiv o deficiență în aplicarea masurilor de protectie stabilite prin politica de securitate ce poate fi pusă în evidență și documentată corespunzător;

Incident de securitate – prin incident se va înțelege orice eveniment, în legătură cu un sistem informatic, ale cărui consecințe pot afecta în mod negativ securitatea cibernetică a acestuia.

Integritate – principiul securităţii informaţiei, care asigură acurateţea şi integritatea informaţiilor şi ale metodelor de procesare şi stocare.

Resurse informaționale – totalitatea datelor și informațiilor manipulate în cadrul instituției, procesate cu sau fără ajutorul sistemului informatic şi de comunicaţii.

Reţea – reprezintă o structură interconectată de echipamente de comunicație (hub, router, switch etc.) și terminale (stații de lucru, telefoane, servere etc.) având ca scop utilizarea în comun a unor resurse software, dispozitive de intrare-ieşire, date şi voce.

Serviciu – o componentă software care rulează în fundal (background) pe un sistem informatic (adesea server) și răspunde la cererile clienților (utilizatori, aplicații client etc.).

Sistemul informatic şi de comunicaţii – reprezintă un sistem prin intermediul căruia se realizează colectarea, transmiterea, stocarea și prelucrarea informației în format electronic. Un sistem informatic poate avea diferite componente: calculatoare, dispozitive de rețea, medii de transmisie, aplicații informatice, tehnologii de securitate și chiar utilizatori.

Utilizator – este persoana căreia i s-au conferit în mod legal drepturi de acces la sistemul informatic și de comunicații electronice al instituției.

7. Sugestii de îmbunătățire și raportare incidente

Prezentul ghid se dorește a fi un „live document", actualizat în permanență, odată cu evoluția tehnologiilor IT&C și a amenințărilor din spațiul cibernetic, dar și în baza observațiilor și propunerilor de îmbunătățire primite de CERT-RO.

În acest sens, CERT-RO încurajează specialiștii și utilizatorii de sisteme IT&C să contribuie la îmbunătățirea acestui ghid prin transmiterea sugestiilor la adresa de email sugestii@cert.ro.

De asemenea, **CERT-RO**, în calitate de instituție publică cu atribuții în prevenirea, analiza, identificarea și reacția la incidentele produse în cadrul infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori servicii ale societății informaționale, **vă recomandă raportarea incidentelor de securitate la adresa de email alerts@cert.ro, sau telefon +40-316.202.164**.

8. Bibliografie

1. "Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior", comunicat de presă, 24 iunie 2013
2. "Ghid de protecție a terminalelor mobile în vacanță. Principalele probleme care pot apărea sunt furtul sau pierderea dispozitivelor sau descărcarea de aplicații ce conțin viruși", comunicat de presă Bitdefender, 30 iulie 2013
3. "10 pași pentru îmbunătățirea securității unui calculator nou", RoCSIRT 13 august 2012 – https://www.csirt.ro/files/articles/20120814%20-%2010%20pasi%20pentru%20imbunatatirea%20securitatii%20unui%20calculator%20nou.pdf
4. " Small Office/Home Office Router Security", US-CERT 2011 – https://www.us-cert.gov/sites/default/files/publications/HomeRouterSecurity2011.pdf
5. " Socializing Securely: Using Social Networking Services", US-CERT 2011 – https://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf
6. " Securing Your Web Browser" – https://www.us-cert.gov/publications/securing-your-web-browser
7. "Technical Trends in Phishing Attacks" — http://www.cert.org/archive/pdf/Phishing_trends.pdf

8. ”Spyware” — http://www.cert.org/archive/pdf/spyware2005.pdf
9. ”Before You Connect a New Computer to the Internet” — http:///www.us-cert.gov/security-publications/you-connect-new-computer-internet
10. ”Home Network Security” — http:///www.us-cert.gov/security-publications/home-network-security
11. ”Understanding Your Computer: Web Browsers” — http://www.us-cert.gov/ncas/tips/st04-022-0
12. ”Evaluating Your Web Browser's Security Settings” — http://www.us-cert.gov/ncas/tips/st05-001
13. ”Understanding Website Certificates” — http://www.us-cert.gov/ncas/tips/st05-010
14. ”Avoiding Social Engineering” — http://www.us-cert.gov/ncas/tips/st04-014
15. ” Securitatea sistemelor informatice - a utilizatorilor - si a reţelelor” – http://www.mygarage.ro/ghiduri-si-tutoriale/134275-ghid-securitate-sistemelor-informatice-utilizatorilor-si-retelelor.html
16. ” Securitatea rețelelor de calculatoare” – https://ro.wikipedia.org/wiki/Securitatea_re%C8%9Belelor_de_calculatoare
17. ” Ghid de protecție a terminalelor mobile în vacanță” – http://www.securitatea-informatiilor.ro/stiri-de-ultima-ora/ghid-de-protectie-a-terminalelor-mobile-in-vacanta/
18. ” Mic ghid de securitate a datelor pentru companii mici și mijlocii” – http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/mic-ghid-de-securitate-a-datelor-pentru-companii-mici-si-mijlocii/
19. ” Protejeaza-ti datele transmise de pe telefon prin retelele WiFi publice” – http://www.securitatea-informatiilor.ro/stiri-de-ultima-ora/cum-folosesti-in-siguranta-retelele-publice-de-wifi/
20. ”Cum foloseşti în siguranță reţelele publice de WiFi” – http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/securitatea-datelor/protejeaza-ti-datele-transmise-de-pe-telefon-prin-retelele-wifi-publice/#more-1590
21. ” Asigurarea securității informațiilor” – http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/asigurarea-securitatii-informatiilor/
22. ”Cum te ferești de atacurile informatice de pe e-mail” – http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/cum-te-feresti-de-atacurile-informatice-de-pe-e-mail/
23. ”10 semne de infectare a computerului” – http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/10-semne-de-infectare-a-computerului/
24. ” GHID - Securitatea terminalelor mobile” – https://www.cert.ro/files/doc/797_20131114101154003203000_X.pdf
25. ” Ghid de bune practici pentru securizarea calculatoarelor și rețelelor personale” – https://www.cert.ro/files/doc/728_20130401030442003008400_X.pdf

26. ” GHID - Securitatea în rețele sociale şi controlul parental în mediul online” – https://www.cert.ro/files/doc/790_20131114101124026571900_X.pdf
27. ” GHID - privind securitatea serviciilor Internet Banking și Online Shopping” – https://www.cert.ro/files/doc/793_20131114101135013176000_X.pdf
28. ”GHID - Cum să te ferești de viruși, viermi și troieni” – https://www.cert.ro/files/doc/788_20131114101131020771200_X.pdf
29. ” GHID - Securitatea utilizatorului final” – https://www.cert.ro/files/doc/795_20131114101128009452200_X.pdf
30. ” GHID - Amenințări generice la adresa securității cibernetice” – https://www.cert.ro/files/doc/789_20131114101107065907800_X.pdf
31. ” Cod de bune practici pentru Securitatea Sistemelor Informatice și de Comunicații” – https://www.cert.ro/files/doc/729_20130401030415043075400_X.pdf.