European Commission

eSKILLS FOR JOBS 2015

APDETIC
Asociația Producătorilor și Distribuitorilor de Echipamente de Tehnologia Informației și Comunicațiilor

e-ghid pentru securitate cibernetică

POLIȚIA ROMÂNĂ

European Commission

Grand Coalition for Digital Jobs

e-ghid pentru securitate cibernetică

"Securitatea cibernetica a devenit in ultimii ani o prioritate maxima pentru toti utilizatorii din lume.
Cresterea prezentei tehnologiei digitale in toate sferele societatii actuale a intarit nevoia de a adopta si implementa masuri de prevenire si protejare a activitatilor multiple care au loc zilnic si care implica miliarde de utilizatori.
In contextul campaniei europene de constientizare eSkills for jobs (Competente digitale pentru locuri de munca) , APDETIC, impreuna cu partenerii sai, Av. Magda Popescu, Politia Romana, prin Institutul de Cercetare si Prevenire a Criminalitatii, si Cisco Romania, a elaborat, un Ghid de Securitate cibernetica, ce isi propune sa ofere o importanta baza de informare, recomandari si sfaturi utile pentru contracararea riscurilor si amenintarilor informatice."

Valentin Negoita, Presedinte APDETIC

Autori:
Avocat Magda Popescu
Asociatia producatorilor de echipamente de tehnologia informatiei si comunicatiilor (APDETIC)
Institutul de Cercetare si Prevenire a Criminalitatii din cadrul Inspectoratului General al Politiei Romane

INTRODUCERE

În cadrul programului european E-skills[1], Asociația Producătorilor și Distribuitorilor de Echipamente de Tehnologia Informației și Comunicații - APDETIC, în colaborare cu Poliția Română – Institutul de Cercetare și Prevenire a Criminalității și Cisco România, prezintă e-ghidul pentru securitate cibernetică – o introducere generală, cu informații de bază referitoare la amenințările de securitate cibernetică și la metodele primare de prevenire și combatere a acestora.

În prezent, criminalitatea cibernetică este în continuă creștere – foarte multe atacuri, intruziuni și alte activități ilicite se mută din spațiul fizic în cel online. Deopotrivă activități curente de fraudă și operațiuni sofisticate de furt de identitate, de date și informații sensibile sau terorism cibernetic se desfășoară în noul "El Dorado" – Internetul și spațiul cibernetic.

O altă zonă importantă de risc este reprezentată de obiectele fizice – automobile, echipamente industriale, echipamente electrocasnice și electronice de uz profesional sau personal, ce au sisteme de operare și aplicații informatice embedded – care sunt conectate la rețeaua informatică (așa numitul "Internet al Lucrurilor" – "Internet of Things"). Conexiunea între miliarde de astfel de echipamente și sistemele IT și operaționale deschide poarta unui nou univers ce poate fi vulnerabil la riscuri de securitate cibernetică.

Având în vedere aceste amenințări, nu este de mirare că un survey realizat, în 2014, de PriceWaterhouseCoopers, la nivelul CEO, a relevat că pericolele sunt deja conștientizate, cel puțin în zona de business – 49% din CEO intervievați la nivel global și-au exprimat îngrijorarea cu privire la amenințările cibernetice la adresa potențialui de creștere a business-ului. De asemenea, zona guvernamentală este conștientă de aceste amenințări, din ce în ce mai mult fiind recunoscute ca probleme de securitate națională.

Însă, în afară de problemele de impact la nivel înalt, fiecare dintre noi suntem expuși riscurilor – în viața personală sau la serviciu. Cel mai recent raport de securitate al Symantec[2] arată că:

- 60% dintre atacurile cibernetice din 2014 au vizat organizații mici și mijlocii, mai vulnerabile din cauza resurselor limitate pe care le au la dispoziție pentru a investi în securitate. Cu toate acestea, riscurile depășesc granița organizației atacate, putând afecta totodată clienții, partenerii de afaceri ai acestora, angajații etc.
- Există peste 317 milioane de noi coduri malițioase (malware) create în 2014, deci aproape un milion zilnic.
- Atacurile de tip ransomware au crescut cu 113 procente în 2014, iar atacturile de tip ransomware bazate pe criptarea informațiilor victimelor – cu 4.000 de procente.

---

[1] Comisia Europeană a selectat DIGITALEUROPE pentru a organiza Campania eSkills for jobs (Competențe digitale pentru locuri de muncă) în 2015. Campania este organizată sub umbrela Marii Coaliții pentru locuri de muncă bazate pe competențe digitale lansată de Comisia europeană, un larg parteneriat pan-european menit să contribuie la reducerea deficitului de cetățeni europeni cu competențe profesionale digitale și de a valorifica potențialul de creare de locuri de muncă în sectorul ITC. Campania va informa elevii si studenții, oamenii aflati in cautare de joburi, profesioniștii din sectorul ITC si IMM-urile despre marea varietate de oportunități pe care o prezinta locurile de muncă bazate pe tehnologia informației si comunicațiilor. Ca membră a organizației internationale DIGITALEUROPE, A.P.D.E.T.I.C. coordonează în România activitatile Campaniei eSkills for jobs 2015.

[2] Symantec 2015 Internet Security Threat Report
http://www.symantec.com/security_response/publications/threatreport.jsp

- Atacurile de tip ransomware au crescut cu 113 procente în 2014, iar atacturile de tip ransomware bazate pe criptarea informațiilor victimelor – cu 4.000 de procente.
- Dintre vectorii utilizați de atacatori, emailul rămâne foarte folosit, dar se remarcă și o creștere a activității ilicite prin intermediul platformelor de socializare. În 2014, 70% din scam-urile ce au circulat pe social media au fost răspândite manual.
- Mobilul devine, de asemenea, din ce în ce mai mult, o sursă de vulnerabilitate, pentru că tradițional oamenii percep PC-ul ca fiind mediul de atacuri cibernetice, ignorând telefonul mobil. Cu toate acestea, în 2014, 17% din aplicațiile pentru Android erau de fapt malware.

Prima persoană responsabilă pentru prevenirea și combaterea riscurilor este chiar persoana (fizică sau juridică) expusă acestora. Tehnologia este un instrument care ne face viața mai ușoară și nu avem niciun motiv să renunțăm la ea – trebuie doar să fim conștienți de pericole și să luăm măsuri. Problema securității cibernetice poate părea descurajant de dificilă și complicată, dar poate fi abordată pas cu pas. Securitatea informatică variază de la simpla securitate fizică (de pildă, asigurându-vă că laptop-uri și alte suporturi portabile sunt asigurate atunci când nu sunt folosite) până la a pune în aplicare sisteme mai sofisticate (firewall-uri, sisteme de detectare și de prevenire a intruziunilor, software antivirus și anti-spyware).
Soluțiile pot fi low-cost și simplu de implementat sau cu costuri ridicate și complexe ori într-o zonă intermediară. Primul pas este identificarea problemei și punerea în aplicare a unui mix de soluții care să răspundă cel mai bine nevoilor persoanei sau companiei.

Din acest motiv, ghidul vă propune o scurtă trecere în revistă a problemelor de cyber-security. El nu reprezintă un studiu sau un instrument sofisticat, după lecturarea căruia să deveniți specialiști în contracararea atacurilor cibernetice, însă vă poate prezenta și atrage atenția asupra unor pași simpli și accesibili, care, însă, pot face o mare diferență.

I.CARE SUNT PERICOLELE ȘI CÂT DE EXPUȘI SUNTEM

O mare varietate de situații pot fi calificate ca incidente de securitate cibernetică:

- Website-ul companiei poate fi compromis sau poate deveni indisponibil;
- Computerul/computerele sau alte echipamente devin nefuncționale din cauza malware-ului;
- Furtul de date – de identitate, bancare, personale ale angajaților sau clienților, informații de afaceri, pentru a fi utilizate direct de atacator sau pentru a-și însuși identitatea victimei, la adăpostul căreia atacatorul derulează operațiuni frauduloase;
- Alterarea sau distrugerea datelor;
- Infectarea computerului/rețelei și utilizarea acestora pentru atacarea altor sisteme;
- Stocarea neautorizată, pe computerul victimei, de fișiere ale atacatorului, inclusiv în situații de file-sharing, de materiale neautorizate (muzică pirat, filme pirat etc.) de pe computerul-victimă.

Există multe posibilități prin care persoane neautorizate pot accesa un sistem sau o rețea:

- Trojeni – programe ce au un scop malițios ascuns; pot, de asemenea, instala alte feluri de malware sau back-doors;
- Backdoors – malware care permite atacatorului să controleze de la distanță computerul victimei;
- Key-loggers – software care înregistrează mișcările tastaturii și, astfel, poate colecta user id, parole, numere și date de carduri bancare etc., pe care le transmite atacatorului.

Incidentele de securitate cibernetică intervin, de regulă, în contextul conexiunii la Internet, însă pot fi vulnerabile și sistemele aflate offline.

Un computer neprotejat conectat la Internet poate fi compromis în mai puțin de un minut. Un computer infectat sau compromis conectat la alte computere neprotejate poate foarte ușor și rapid să transmită codul malițios sau poate fi punctul de intrare neautorizată în rețea.

Chiar și un computer nelegat la Internet poate fi vulnerabil. Un sistem neprotejat poate fi accesat fizic de persoane neautorizate sau poate fi infectat prin suporturi sau dispozitive infectate (CD, DVD, USD/flash drive etc.).

II.CE PUTEM FACE – 10 PAȘI PENTRU A FI MAI SIGURI

II.1. ÎNVĂȚAȚI SĂ RECUNOAȘTEȚI O PROBLEMĂ DE SECURITATE INFORMATICĂ ATUNCI CÂND APARE

Primul pas spre rezolvarea unei probleme este recunoașterea ei. Un dispozitiv (computer, telefon etc.) ar putea avea o problemă de securitate informatică atunci când:

- Funcționarea încetinește sau chiar se oprește;
- Apar situații neașteptate, cum ar fi pornirea spontană a unor programe;
- Apar indicii de activitate intensă a hard-disk-ului, deși utilizatorul legitim nu a generat astfel de procese;
- Apariția unor mesaje noi;
- Alertă bruscă de insuficiență a spațiului de pe disc;
- Imposibilitatea de rulare a unui program din cauza memoriei insuficiente (dacă este o situație apărută neașteptat);
- Disfuncționalități frecvente;
- Detectarea conectării automate la alte computere, care nu a fost autorizată și nu are legătură cu uzul personal sau profesional al computerului;
- Returul e-mailurilor (bounce-back);
- Nu se mai primesc emailuri;
- Website-ul companiei sau al persoanei respective nu mai are vizitatori;
- Se primesc sesizări de la utilizatori că credențialele de conectare (nume de utilizator și parole) nu mai funcționează;
- Se primesc sesizări de la utilizatori că rețeaua este neașteptat de încetinită în funcționare;
- Sunt reclamații de la utilizatori care primesc informații în sensul că PC-ul lor este infectat ori de câte ori accesează site-ul victimei;
- Extrasul de cont bancar folosit online indică operațiuni suspecte sau de care titularul nu își amintește;
- Numele și datele de identificare ale victimei apar pe site-uri sau chiar documente ce nu au fost autorizate de titular (de exemplu, pentru abonarea la site-uri, obținerea de credite, derularea unor operațiuni online, pe site-uri de dating etc.).

II.2. STABILIȚI PAȘII DE URMAT PENTRU A REZOLVA O PROBLEMĂ DE SECURITATE INFORMATICĂ

- În primul rând, învățați să recunoașteți rapid și cât mai devreme o problemă de securitate cibernetică (a se vedea și capitolul anterior);
- Scoateți cât mai rapid din funcțiune și/sau deconectați echipamentul infectat ori compromis pentru a preveni escaladarea incidentului;
- Informați managerul, în cazul în care problema se întâmplă la serviciu sau pe un echipament de serviciu, și/sau ceilalți utilizatori cu care ați fost în contact prin intermediul acelui dispozitiv infectat sau compromis;

- În cazul în care prin intermediul echipamentului infectat sau compromis ați comunicat cu parteneri de afaceri și/sau clienți, consultați-vă întotdeauna cu managerul dvs. înainte de a-i contacta pe aceștia;
- Contactați autoritățile competente atunci când apreciați că este vorba de o activitate ilicită de criminalitate informatică. Conform legislației române, reprezintă fapte penale următoarele:
- Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic;
- Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia;
- Falsul informatic – adică introducerea, modificarea sau ștergerea, fără drept, de date informatice ori restricționarea, fără drept, a accesului la aceste date, rezultând date necorespunzătoare adevărului;
- Accesul, fără drept, la un sistem informatic;
- Interceptarea, fără drept, a unei transmisii de date informatice ce nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic;
- Interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice;
- Modificarea, ștergerea sau deteriorarea de date informatice ori restricționarea accesului la aceste date, fără drept;
- Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice;
- Transferul neautorizat de date dintr-un sistem informatic sau mijloc de stocare a datelor informatice;
- Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă: (i) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre faptele de mai sus; (ii) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre faptele de mai sus;
- Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice similare, în scopul săvârșirii uneia dintre faptele de mai sus;
- Tentativa la infracțiunile enumerate se pedepsește.
- Rezolvați problema (eventual apelând la un specialist) și refaceți funcționarea echipamentului și datele de pe acesta;
- Învățați din greșeli – faceți o evaluare a situației *post-factum*, încercați să determinați comportamentul neglijent sau riscant ce a permis incidentul și luați măsuri de îmbunătățire pentru viitor a nivelului de securitate cibernetică.

II.3. PROTEJAȚI ECHIPAMENTUL DIN PUNCT DE VEDERE FIZIC

- Computerul, ca și orice alte dispozitive care conțin date importante sau permit accesul la date importante, trebuie să fie protejat fizic cu privire la incidente de securitate, accidente, calamități, precum și contra accesului neautorizat în vederea sustragerii sau simplei accesări ori deteriorări;
- În cazul în care călătoriți cu laptopul, tableta, telefonul etc., nu îl predați la bagaje; țineți-l tot timpul cu dumneavoastră sau păstrați-l într-un loc sigur și/sau greu accesibil fără autorizarea dumneavoastră;
- Folosiți un UPS, precum și un protector pentru supratensiune, care să vă protejeze de variațiile de tensiune;
- Accesul fizic la echipamente trebuie să fie controlat, cu atât mai mult cu cât e vorba de echipamente critice; accesul la astfel de echipamente ar trebui restricționat chiar și în interiorul organizației, fiind permis doar persoanelor strict autorizate.

II.4. CONTROLAȚI ACCESUL

- Fiecare utilizator care se conectează la un computer sau la o rețea, inclusiv în cloud, trebuie să aibă propriul login unic (user id) și parolă, pentru a se putea ține evidența clară a accesărilor sistemului sau rețelei;
- Alegeți parole puternice – parolele ar trebui să aibă cel puțin 10 caractere, să include litere mari și litere mici, numere și simboluri. Evitați folosirea de cuvinte comune sau personale – nume de familie, prenume, numele câinelui etc., sau alte cuvinte sau combinații care pot fi ușor asociate cu dumneavoastră;
- Schimbați des parolele;
- În cazul în care aveți vreo bănuială cu privire la accesarea neautorizată a unui cont, schimbați parola și contactați furnizorul sau specialistul IT pentru a încerca să vă modificați chiar și contul;
- În cazul în care aveți o bănuială sau certitudine cu privire la accesarea neautorizată a unei parole asociate unui anumit cont și folosiți aceeași parolă sau parole asemănătoare și pentru alte conturi, schimbați-le pe toate;
- În cazul în care dispozitivul este localizat sau folosit (dacă este un echipament mobil) într-un spațiu în care au acces sau circulă persoane neautorizate sau în locuri publice, aveți grijă ca ecranul să nu fie vizibil;
- Blocați-vă dispozitivul sau computerul atunci când nu îl utilizați sau nu sunteți prin preajmă, astfel încât să se solicite user id și parola pentru orice deblocare sau reinițiere a utilizării (în mod normal, se poate seta și o funcție de blocare automată după un anumit interval de timp de neutilizare sau se poate folosi combinația rapidă de taste control+alt+delete);
- Nu setați opțiunea de memorare automată a parolelor;
- Implementați o procedură aplicabilă în cazul încetării colaborării cu angajații – predarea laptopului, a telefonului mobil etc., dezactivarea contului și parolei, dezactivarea drepturilor de acces, schimbarea parolelor pentru conturile ce nu pot fi dezactivate. Această procedură ar trebui aplicată inclusiv atunci când un angajat nu părăsește compania, ci doar departamentul sau felul activității, de natură a modifica însă drepturile de acces și/sau zonele la care i se permite accesul, inclusiv în mediul informatic.

II.5. PROTEJAȚI SOFTWARE-UL ȘI HARDWARE-UL ESENȚIAL

- Instalați, configurați și utilizați firewall-ul;
- Instalați software anti-virus și anti-spyware și asigurați-vă că se updatează periodic și cât mai des. Rețineți că existența firewall-ului nu suplinește programul anti-virus;
- Setați toate dispozitivele pe care le utilizați pe funcția auto-update pentru a vă asigura că aveți ultimele patch-uri de securitate.

Câteva cuvinte în plus despre firewall-uri

Firewall-ul este un program pentru calculator sau un dispozitiv hardware care filtrează informația ce circulă între un sistem sau rețea, pe de o parte, și Internet, pe de altă parte. Firewall-ul este necesar, dar nu suficient pentru securitatea computerului sau rețelei. Chiar și dacă are un firewall, există în continuare riscul ca un computer să fie atacat – de pildă, dacă nu există antivirus sau acesta nu este updatat, iar prin email se primește un mesaj infectat, acesta poate infecta calculatorul.

Software firewall – este un program care se instalează și rulează în mod direct pe calculator. Nivelul de securitate stabilit pentru firewall determină cât din traficul de pe Internet urmează a fi oprit; desigur, nu poate fi oprit întregul trafic, pentru că acest lucru ar face inutilizabilă conexiunea la Internet. Sfaturi de instalare și utilizare a unui software firewall:

- Majoritatea software-urilor firewall utilizează un ”wizard” de instalare care îl conduce pe utilizator în acest proces. Ori de câte ori nu sunteți siguri ce să răspundeți, alegeți varianta ”default” sau ”recommended”.
- Când sunteți întrebați dacă se configurează o rețea, răspunsul ar trebui să fie ”nu”, în cazul în care e vorba de un singur computer.
- Atunci când există o funcție de update automat, activați-o.
- Asigurați-vă că aveți ultima versiune de firewall disponibilă.
- Activați funcția de jurnal (logging); urmărirea acestora vă poate indica activitățile suspecte din rețeaua dumneavoastră.
- Odată instalat, firewall-ul alertează utilizatorul la prima încercare de accesare a Internetului de către o aplicație. Dacă este vorba de o aplicație pe care o cunoașteți, selectați ”allow” sau ”do not block”. Dacă este vorba despre o aplicați pe care nu o recunoașteți, rulați o căutare pe Internet (Google, Bing etc.) și încercați să aflați mai multe despre aplicația respectivă. În cazul în care ceva vi se pare suspect sau nu sunteți lămuriți, selectați opțiunea ”do not allow”, ”block”, ”deny” etc.

Wired hardware firewall – este un echipament cu fir și operarea lui solicită un nivel de pregătire tehnică ceva mai ridicat. Contactați un specialist înainte de a întreprinde oricare din modificările/acțiunile recomandate mai jos:

- Schimbați parola default într-o parolă dificil de identificat; nu păstrați parola default întrucât nu știți cu siguranță cine o mai are.
- Dezactivați opțiunea de gestionare la distanță (”remote management”); altfel vă expuneți riscului ca firewall-ul să fie configurat de la distanță de o persoană neautorizată.
- Activați exclusiv opțiunile din firewall care permit rularea aplicațiilor ce au nevoie de conexiune la Internet.

- Activați funcția de jurnal (logging); urmărirea acestora vă poate indica activitățile suspecte din rețeaua dumneavoastră. De pildă, dacă observați că un calculator din rețeaua de la birou s-a conectat la Internet noaptea, când nu era nimeni la lucru, s-ar putea să fie vorba de un virus sau de un acces neautorizat; asigurați-vă totuși că nu e vorba de update-uri automate de software înainte de a merge mai departe.

Wireless hardware firewall – este un echipament fără fir, ceea ce face operarea sa puțin mai complicată. În plus față de cele de mai sus, există următoarele recomandări:

- Activați opțiunea de filtrare a adresei MAC pentru a vă asigura că numai computerele din rețeaua dumneavoastră se conectează la firewall-ul respectiv. Când configurați firewall-ul, introduceți adresele MAC ale fiecărui computer ce are autorizare de conectare la rețea – adresa MAC se găsește pe adaptorul wireless al computerului sau poate fi găsit în utilitarul care e folosit pentru rularea adaptorului wireless.
- Activați opțiunea de criptare a informației transmise între computer și firewall în conexiunea wireless; accesul în acest caz se face cu cheie/parolă.
- Este recomandabilă utilizarea SSID-urilor criptate, inclusiv acasă, pentru a preveni situația posibilă ca un atacator să se plaseze în apropiere și astfel să poată intercepta tot traficul. osiți aceeași parolă sau parole asemănătoare și pentru alte conturi, schimbați-le pe toate;
- Utilizați pentru autentificare protocolul WPA2, iar nu WEP, acesta fiind un protocol compromis deja.

II.6. PROTEJAȚI-VĂ INFORMAȚIA

- Faceți în mod regulat back-up la informații;
- Instalați în mod regulat patchurile de sistem de operare și software;
- Aveți grijă cu dispozitivele portabile de mici dimensiuni – CD-uri, DVD-uri, memory-stick-uri etc. Pot avea o mulțime de informații și se pot pierde sau subtiliza ușor;
- Aveți grijă la site-urile de Internet vizitate. Unele site-uri pot:
- Să vă redirecționeze către site-uri pe care nu intenționați să le vizitați;
- Să vă solicite informații personale care pot fi folosite în furt de identitate;
- Să genereze infectarea cu malware.

Câteva cuvinte în plus despre back-up

Back-up-ul este o copie a datelor în format electronic destinată a fi utilizată în cazul în care originalul este pierdut sau deteriorat.

Cantitatea de informație cu care se lucrează zilnic în format electronic este imensă. Se pune întrebarea cât din această trebuie să aibă și back-up; de fapt, întrebarea corectă este – câtă informație vă puteți permite să pierdeți? Indiferent de răspuns, atenție la faptul că și fișierele și setările software-ului și aplicațiilor trebuie să fie incluse în back-up, pentru a permite o reconfigurare rapidă a sistemelor, în caz de probleme.

Back-up vs. Arhivare

Back-up-ul este o copie a datelor în format electronic destinată a fi utilizată în cazul în care originalul este pierdut sau deteriorat. Back-up-urile pot fi compresate pentru a câștiga spațiu sau criptate din rațiuni de securitate. Bunele practici de back-up recomandă să existe mai multe versiuni de back-up, pentru a crește șansele de recuperare a informației, precum și ca back-up-urile să fie etichetate.

Arhivarea, pe de altă parte, se referă la păstrarea informației digitale valoroase pentru o organizație, care trebuie păstrată nealterată și accesibilă pe o anumită perioadă de timp. Arhivarea presupuse existența unei copii master și a cel puțin unui duplicat, păstrat în altă locație decât masterul. Bunele practici de arhivare recomandă ca informația să nu fie compresată sau criptată (cu excepția informațiilor foarte sensibile), întrucât s-ar putea astfel limita capacitatea organizației de a accesa și utiliza acele date în viitor. De asemenea, bunele practici de arhivare impun migrarea sau refreshingul suporturilor, de regulă o dată la 3 ani și în orice caz la 5 ani, întrucât condițiile climatice și reutilizările pot uza suporturile și le pot face neutilizabile. De asemenea, se recomandă să se utilizeze formate de fișiere larg răspândite și neproprietare, pentru a se evita situația în care formatul nu mai este disponibil pe piață la momentul în care este nevoie să fie accesate datele.

Procesul de back-up:

1. **Frecvența și tipurile de back-up**

Full back-up – back-up-ul complet, în care se copiază toate informațiile de pe sistem. Acesta este bine să se facă cel puțin săptămânal și se recomandă să fie programate în afara

Back-up incremental – se copiază toate fișierele care au fost create sau modificate de la ultimul back-up, de orice fel ar fi acesta. Se recomandă ca cel puțin un back-up incremental să fie făcut zilnic, iar fișierele de back-up incremental să fie păstrate cel puțin până la următorul back-up full.

Back-up diferențial – se copiază toate fișierele care au fost create sau modificate de la ultimul back-up full.

2. **Verificați informația ce face obiectul back-up-ului și capacitatea de refacere a datelor**

Este recomandabil să verificați periodic dacă informația a fost copiată în back-up în mod corect – verificați existența anumitor informații importante sau prin sondaj, comparați mărimea fișierelor inițiale cu cele aflate pe suportul de back-up.

De asemenea, verificați că informația nu a fost deteriorată între timp și schimbați suporturile de back-up pentru a evita problemele tehnice cu acestea.

3. **Păstrați suporturile pe care aveți back-up-ul în loc sigur**

Una dintre greșelile clasice este de a păstra back-up-urile în același loc unde se află datele originale. În acest caz, orice risc ar afecta datele originale (ex. incendiu, inundație, furt etc.) poate la fel de bine să afecteze și back-up. Așadar, back-up-urile trebuie păstrate în altă locație, pentru care însă se recomandă instituirea de restricții de acces identice, pentru a preveni furtul sau copierea neautorizată a informațiilor.

II.7. ASIGURAȚI-VĂ CĂ ELIMINAȚI ÎN MOD CORECT DATELE DE PE ECHIPAMENTELE PE CARE SUNT STOCATE

Computerele și suporturile pe care sunt stocate date informatice trebuie să fie eliminate într-o manieră care să prevină accesarea neautorizată a datelor care se află sau s-au aflat pe acestea.

Simpla ștergere a fișierelor nu este de natură să elimine definitiv informația. Informația care a fost ștearsă de pe un computer poate fi recuperată prin instrumente de cyber-forensics și alte instrumente.

Din acest motiv, trebuie să se apeleze la mijloace de natură a conduce la eliminarea definitivă și nerecuperabilă a informației. Fie puteți folosi una din metodele enumerate mai jos, fie apelați la un specialist.

1. Metoda wiping – procesul de scriere peste spațiul unde se află datele a căror eliminare se urmărește cu alte date, fără caracter sensibil.

   Dezavantaje: poate dura mult; nu este posibilă pentru echipamente cu defecțiuni; nu este posibilă pentru echipamentele care nu permit rescrierea; în unele cazuri este nevoie de anumite setări tehnice suplimentare.

   Se poate folosi pentru: hard-disk-uri interne și externe, faxuri, printere, copiatoare, multifuncționale, memory-stick-uri, tablete și telefoane etc.

2. Metoda demagnetizării – utilizarea unui magnet foarte puternic pentru ștergerea informației.

   Dezavantaje: magneții puternici utilizați pot afecta toate echipamentele aflate într-o anumită rază, deci aplicarea metodei necesită spațiu și izolare; persoanele purtătoare de pacemaker nu pot aplica metoda; suportul demagnetizat devine permanent neutilizabil.

   Se poate folosi pentru: hard-disk-uri interne și externe etc.

3. Metoda distrugerii fizice – echipamentul este pur și simplu distrus; există shreddere pentru CD-uri/DVD-uri sau, în cazul în care nu dețineți un astfel de instrument sau nu se pretează pentru echipamentul ce trebuie eliminat, puteți apela la ardere, zdrobire, rupere, găurire etc.

   Dezavantaje: probleme de mediu în cazul incinerării; probleme de protecția muncii; trebuie să vă asigurați personal că cel căruia i-a fost încredințată distrugerea chiar a făcut-o și nu a copiat nimic înainte.

   Se poate folosi pentru: hard-disk-uri interne și externe, faxuri, printere, copiatoare, multifuncționale, CD-uri, DVD-uri, memory-stick-uri, tablete și telefoane etc.

Situația echipamentelor aflate în garanție – în cazul în care echipamentul cedează pe perioada garanției, în mod normal trebuie returnat vânzătorului pentru a primi altul nou. Cu toate acestea, s-ar putea ca date sensibile sau confidențiale să se afle în continuare pe echipamentul sau suportul defect. În aceste condiții, trebuie să negociați, încă de la momentul cumpărării echipamentului, că returnarea acestuia în caz de folosire a garanției se face doar după eliminarea informației după o metodă acceptată (inclusiv distrugere fizică).

Mai mult, vă recomandăm să păstrați evidența echipamentelor și suporturilor distruse, care să includă echipamentul, producătorul, serialul, metoda de eliminare folosită, data eliminării.

II.8. DESEMNAȚI O PERSOANĂ RESPONSABILĂ PENTRU SECURITATEA INFORMATICĂ (PENTRU COMPANII)

Numiți, prin act intern scris, o persoană care să fie responsabilă pentru securitatea cibernetică pentru a vă asigura că sunt implementate proceduri și politici adecvate. Această muncă poate fi full time sau cu timp parțial, în funcție de complexitatea și tipul operațiunilor derulate în cadrul organizației;

- Definiți clar atribuțiile de securitate cibernetică în fișa postului acestei persoane;
- Asigurați-vă că țineți la zi inventarul hardware și software; nu neglijați dispozitivele de mici dimensiuni și dispozitivele pentru back-up-ul informațiilor;
- Întocmiți un plan de asigurare a securității cibernetice;
- Stabiliți care dintre activele companiei necesită protecție și implementați proceduri adecvate;
- Stabiliți proceduri de răspuns la incidentele de securitate cibernetică;
- Întocmiți planuri de back-up care să asigure continuarea derulării operațiunilor critice de business;
- Puneți în aplicare un program de instruire și informare în materie de securitate cibernetică;
- Stabiliți procedurile de comunicare în caz de incidente de securitate cibernetică, astfel încât fiecare angajat să știe ce, cum și cui să raporteze un astfel de incident sau problemă;
- Asigurați-vă că respectați normele legale referitoare la protecția informațiilor.
    - În România sunt în vigoare Legea 677/2001, privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, precum și Legea 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

II.9. IMPLEMENTAȚI O POLITICĂ REFERITOARE LA DREPTURI DE ACCES ȘI UTILIZAREA INTERNETULUI (PENTRU COMPANII)

Atunci când angajații se conectează la Internet sau trimit emailuri utilizând echipamentele și resursele companiei, ar trebui să facă acest lucru doar în scopurile autorizate de către angajator. Enumerăm în continuare o listă exemplificativă de comportamente generatoare de risc și care pot conduce la incidente de securitate informatică.

Astfel, Internetul și emailul nu ar trebui folosite:

- Pentru a se prezenta drept altcineva;
- Pentru spam;
- Pentru a încerca accesarea neautorizată a unui sistem sau a unei rețele, indiferent că este din cadrul aceleiași organizații sau dintr-o organizație terță;
- Pentru copierea neautorizată sau furtul de informații în formă electronică;
- Pentru încălcarea unor drepturi de proprietate intelectuală sau a altor drepturi exclusive recunoscute de legislația națională și internațională;
- Pentru transmiterea sau postarea de date și informații ale organizației, fără autorizarea acesteia;
- Pentru a răspândi malware sau pentru a genera atacuri cibernetice, de tipul DDOS (distributed denial of service) etc.

Angajații ar trebui să fie obligați:

- Să nu dea informații cu privire la userid, parole, drepturile de acces pe care le au, nici în interiorul organizației, către persoane neautorizate, nici în exterior;

- Să nu lase echipamentele pe care le folosesc neprotejate cu userid și parolă, să nu permită accesul persoanelor neautorizate în incinta în care se află acestea;
- Să folosească criptarea informațiilor în toate situațiile în care au fost instruiți în mod expres de către superiorul lor în acest sens;
- Să nu deschidă mesaje electronice suspecte;
- Să nu deschidă atașamente executabile sau fișiere comprimate fără a se asigura că știu exact despre ce e vorba, inclusiv prin confirmare de la expeditor cunoscut și/sau cu acordul responsabilului IT;
- Să transmită informațiile sensibile exclusiv criptat;
- Să nu viziteze pagini web ce nu au legătură cu business-ul;

  Să nu dezactiveze setările făcute de administratorul de rețea cu privire la antivirus, anti-spyware, firewall-uri;
- Să nu descarce, să nu instaleze și să nu ruleze software neautorizat;
- Să nu transmită prin platforme de transfer de genul wetransfer, transfer.ro etc. informații sensibile dacă nu sunt criptate;
- Să nu conecteze la echipamentele de birou suporturi și echipamente neautorizate, cum ar fi propriile laptopuri, tablete, telefoane, memory-stick-uri, CD-uri, DVD-uri, mp3-playere, routere wireless etc.;
- Să realizeze back-up-urile stabilite de angajator, la intervalele stabilite, și să asigure păstrarea corespunzătoare a copiilor de back-up;
- Să asigure eliminarea informațiilor în mod efectiv, conform instrucțiunilor angajatorului.
- Update antivirus/setare updatare automatăZilnicUpdate software anti-spyware/setare updatare automatăZilnicUpdate pentru sistemul de operare și alte programeOri de câte ori sunt puse la dispoziție patch-urileTransmiterea de alerte sau notificări de securitateZilnic sau de câte ori este nevoieBack-up-ul fișierelorZilnicBack-up-uri de tip incrementalZilnicFull back-upSăptămânalModificarea parolelorTrimestrialAudit de securitateAnualÎntocmirea/revizuirea inventarului hardware și softwareAnual sau în momentul efectuării de achiziţiiRevizuirea politicilor de securitate cibernetică Anual Sesiuni de pregătire și informare a angajaților Anual Modificarea drepturilor de acces pentru angajațiLa nevoie/la schimbări sau mutări de personalÎntocmirea și semnarea de NDA-uri (acorduri de confidențialitate) cu angajații și colaboratorii/cocontractanțiiLa momentul începerii activității.

II.10. IMPLEMENTAȚI PROGRAME DE TRAINING ȘI INFORMARE (PENTRU COMPANII)

Informați-vă angajații, precum și managerii, voluntarii, colaboratorii ce folosesc echipamentele companiei sau care au acces la datele companiei cu privire la riscurile de securitate cibernetică și procedurile interne implementate pentru prevenirea și limitarea consecințelor unor asemenea incidente.

III ÎN LOC DE CONCLUZIE
ROADMAP PENTRU SIGURANȚĂ CIBERNETICĂ

ACTIVITATE RECOMANDATĂ	FRECVEN?Ă
Update antivirus/setare updatare automată	Zilnic
Update software anti-spyware/setare updatare automată	Zilnic
Update pentru sistemul de operare si alte programe	Ori de câte ori sunt puse la dispozitie patch-urile
Transmiterea de alerte sau notificări de securitate	Zilnic sau de câte ori este nevoie
Back-up-ul fisierelor	Zilnic
Back-up-uri de tip incremental	Zilnic
Full back-up	Săptămânal
Modificarea parolelor	Trimestrial
Audit de securitate	Anual
Întocmirea/revizuirea inventarului hardware si software	Anual sau în momentul efectuării de achiziții
Revizuirea politicilor de securitate cibernetica	Anual
Sesiuni de pregătire si informare a angajatilor	Anual
Modificarea drepturilor de acces pentru angajati	La nevoie/la schimbări sau mutări de personal
Întocmirea si semnarea de NDA-uri (acorduri de confidentialitate) cu angajatii si colaboratorii/cocontractantii	La momentul începerii activitătii

APDETIC

Asociația Producătorilor
și Distribuitorilor
de Echipamente de
Tehnologia Informației
și Comunicațiilor

www.asociatiait.ro