

Protecție și securitate

Dacă urmărim evenimentele legate de impactul calculatoarelor asupra societății, și ne gândim aici la business, administrativ, guvernamental sau privat, pe primul loc se găsește ideea de protecție și securitate. După statistici, principalul vinovat în problemele de protecție și securitate este resursa umană, mai exact, utilizatorul (48% din problemele de securitatea informației sunt cauzate de utilizatorii care în mod intenționat sau accidental au provocat daune unei organizații).

în utilizarea calculatoarelor

Ce trebuie să știm? Ce trebuie să facem? Așa cum spuneam mai sus, protecția și securitatea trebuie să o privim diferit la nivel de instituție, business și individual. Ideal ar fi să avem politici caracteristice celor trei zone. Partea proastă este că atunci când trebuie să ne rezolvăm problemele, tratăm procesele și tehnologia, uitând de cea de a treia componentă, utilizatorii... iar educarea utilizatorilor este punctul cel mai sensibil. Nu e adevărat că, atunci când avem probleme, primul nostru gând se duce către întrebarea: **Care este cel mai bun antivirus?**, evitând însă cauza.

Dacă este vorba de cauză, eliminăm din start posibilitatea sau "dorința" de a vă face rău singuri. De aceea vom discuta despre ce se poate întâmpla în mod "accidental". Vom pleca de la... cu ce riscuri/amenințări ne putem confrunta...

Riscuri/amenințări

Până la generalizarea utilizării Internetului, zonele principale unde puteau fi întâlnite amenințări le regăseam legate de zonele de soft: BIOS (virusi de boot), Sistem de operare (virusi pentru executabile), Office (virusi de macro). Odată cu Internetul plaja de amenințări s-a lărgit, astfel încât, azi, sub titulatura de malware găsim o listă întreagă de "probleme", iar modalitățile de penetrare au devenit 3D: software, hardware, social. Înainte modul de abordare era clasic: dădeam vina pe virusi... și atât.

Acum lucrurile nu sunt atât de simple – chiar dacă "virusii" ocupă cea mai mare parte din evenimente (peste 50%), modul de utilizare și de comportare vis-à-vis de calculator devine "gaura neagră".



Numărul de atacuri asupra aplicațiilor web înregistrat în prima jumătate a anului 2011 a depășit deja numărul total de atacuri identificate în 2009 și este cu 65% mai mare decât numărul total de atacuri măsurate anul în anul în 2010, conform raportului Cyber Security Risks 2011 realizat de HP Digital Vaccine Labs (DVLabs).

[Sursa:
Devirusare.com]

Dacă analizăm lista de „probleme” apărute în ultima perioadă, observăm că suntem vulnerabili din trei puncte de vedere:

A. EXTERN – Atacurile la care suntem supuși zi de zi

Virus – Un virus de calculator se atașează la un program sau fișier care să îi permită să se răspândească de la un computer la altul. La fel ca și un virus uman, un virus de calculator poate provoca de la efecte ușor enervante la altele ce pot deteriora hardware, software sau fișiere. Aproape toți virușii sunt atașați la un fișier executabil, ceea ce înseamnă că virusul poate exista pe calculatorul dvs., dar se poate infecta computerul doar atunci când rulați sau deschideți programul dăunător. Virușii au nevoie de acțiunea umană pentru a se răspândi (partajarea fișierelor sau trimiterea de emailuri cu virus ca atașament).

Worm – Un vierme este similar cu un virus numai că ei se propagă de la calculator la calculator fără nici o acțiune umană. El se poate reproduce pe sistemul dvs., astfel încât calculatorul dvs. trimite un vierme singur, în sute sau mii de copii (ex. cei care se folosesc de address book din clientul de mail). Se poate observa un consum exagerat de memorie de sistem sau de lățime de bandă de rețea. Într-o altă variantă viermele permite ca cineva să preia controlul computerul de la distanță.

Trojan – La fel ca și în mitologicul Calul Troian, prin intermediul unui fișier sau software ce pare legitim se activează pe computer, iar rezultatele pot varia de la efecte minore (mai mult enervante) la altele grave, cum ar fi ștergerea fișierelor sau chiar distrugerea sistemului dumneavoastră. Ei sunt cunoscuți pentru faptul că realizează un backdoor pe computer (oferă accesul din exterior la sistemul dvs., și astfel să permită, eventual, accesul la informații confidențiale sau cu caracter

personal care urmează să fie compromise). Spre deosebire de viruși și viermi, troieni nu se reproduc prin infectarea altor fișiere și nici nu se vor auto-replica.

Spyware – atașat de obicei la programe gratuite, captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul) și le folosește apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate. Programele spion care nu extrag date de marketing, ci doar transmit reclame se numesc adware.

Rootkit – Un rootkit este un soft, constând în unul sau mai multe executabile, conceput cu scopul de a ascunde utilizatorului faptul că sistemul a fost compromis. Asta-l face extrem de periculos, mai ales că un rootkit este capabil, nici mai mult nici mai puțin, de a prelua controlul sistemului de operare.

Botnet – Cuvântul botnet provine de la robot, aceasta însemnând că calculatoarele îndeplinesc comenzile proprietarului lor. O rețea botnet este o rețea de calculatoare care au fost compromise fără știința utilizatorului și sunt controlate prin IRC cu scopul de a realiza activități rău intenționate cum ar fi de la trimiterea de mesaje spam, la lansarea de atacuri DDOS (Distributed Denial of Services). Rețelele de botnet pot acumula o putere mare de procesare mulțumită execuției distributive a mai multor aplicații create de atacatori și pot lansa mai multe atacuri simultane către un număr mai mare de ținte. Botnet-ul are în spate principiul de la trojan, iar modul de „agățare” e dat de linkuri la fișiere atractive via email, messenger.



8,6%

**Virus
AutorunINF.Gen**

Firma Bitdefender anunța în iulie 2011, pe locul doi în ierarhia amenințărilor informatice din România, cu un procentaj de 8,6%, virusul de tip Trojan, AutorunINF.Gen. De ce este atât de important?

Pentru că el se propagă pe suporturile de stocare de tip Flash USB, folosind “facilitatea” de Autorun a sistemului de operare Microsoft Windows.

B. UTILIZATOR – educarea lor vis-à-vis de modul de comportare în anumite situații

Spam – Nu este virus... ci doar mesaj “comercial” nedorit. Se distinge prin caracterul agresiv și repetitiv. Deschiderea unui mesaj atrage după sine fapt că destinatarul există (în general spam-ul este trimis la adrese în bloc – fără să se știe dacă acestea există sau nu) deci, automat, o înmulțire a numărului de mesaje nedorite. Deci, nu deschideți orice mesaj din Inbox. Oricum, aproape 90% din mailurile primite de o firmă sunt din categoria spam.

Scareware – La navigarea pe Internet pot apare mesaje de tip pop-up care să vă anunțe existența unui virus și instalarea unui program antivirus (în general “free”) pentru scanarea “imediată”. Varianta fericită este ca acest mesaj să te îndrepte către un site cu soft antivirus fals (și atunci sfatul meu este nu descărcați și nu instalați soft pe care nu-l cunoașteți). Varianta mai puțin fericită este că oriunde veți face click în fereastra de pop-up se activează un virus... atunci forțați închiderea browser-ului.

Phishing – Mail-uri sau pop-up-uri ce par a fi surse sigure și care cer informații, în general, confidențiale. Pot fi recunoscute printr-o editare greșită (greșeli de vocabular sau gramaticale) și, sau mai ales, prin link-urile care duc către site ne-conforme (de exemplu, e-mail de la banca BRD cu link către un site rusesc). Atenție! Nu faceți click pe link ci doar vizualizați unde acesta se duce. Sunt și situații “comice”: să primești e-mail de la BancPost să-ți dai date de identificare, dar tu să nu ai cont la această bancă. Deci, nu deschideți linkurile, nu dați informații confidențiale pe net pentru oricine și, mai ales, dacă observați ceva suspect, anunțați instituția respectivă.



Email scam – Email-uri care se folosesc nu numai de naivitatea oamenilor, ci și de dorința de a câștiga “ceva”. Poate mai țineți minte emailurile care vă anunțau de moștenirea din Nigeria... acum se poartă câștigarea la loteria vizelor USA, excursii exotice, mașini etc. Nu răspundeți primului impuls, ci încercați să citiți printre rânduri... dacă tot nu sunteți siguri, întrebați...

Conform unui studiu „Global IT Security Risks” realizat de Kaspersky Lab în parteneriat cu B2B International, un institut specializat în cercetarea de business, peste 90% dintre companii au avut cel puțin un incident informatic... Dintre amenințările informatice enumerate, cele mai populare sunt virușii și spyware-ul.

C. ACHIZIȚIILE – sau mai bine zis ceea ce utilizăm la nivel hardware și software

Hardware depășit – Este un lucru cunoscut că ne achiziționăm calculatorul pe care ni-l permitem dar instalăm softul cel mai nou de pe piață, normal – piratat. Faptul că utilizăm soft nou este un lucru bun, dar dacă nu investim și în hardware pierdem în ceea ce privește atuurile compatibilității. O să vedem mai târziu ce înseamnă asta.

Echipeamente furate sau pierdute – Multe firme nu dau publicității pierderile datorate greșelilor angajaților. Oricum, prin presă mai “transpiră” informații cu echipamente mobile uitate prin parcuri, restaurante sau mijloace de transport. Tot la fel de mai rău este când acestea sunt furate. La pierderea sau furtul lor nu trebuie să calculați numai echipamentul ci și valoare informațiilor din acestea, mai ales dacă sunt confidențiale. Nu trebuie să vă gândiți numai la echipamente de calcul, ci și la suporturi de stocare mobile.

Software neactualizat sau piratat – Nu este de ajuns dacă aveți un sistem de operare sau un antivirus care promit să vă asigure protecția dacă nu verificați și instalați update-urile pentru acesta. Într-adevăr, Microsoft ne “deranjează” cu service pack-urile sau update-urile pentru sistem, dar acestea sunt mai mult decât necesare pentru că rezolvă problemele care apar permanent. Nu mai vorbim de programul antivirus – este un lucru sub-înțeles. În ceea ce privește softul piratat este un risc asumat... “Riști și câștigi”, nu?



Dar să ne întoarcem la ideea de protecție și securitate... Este vreo diferență între cele două (asta e o întrebare interesantă de pus celor din IT)? Normal că există, dar depinde cum le tratăm. Hai mai bine să vorbim despre Politici de securitate și Mijloace și metode de a asigura protecția.

Politici de securitate

Politicile de securitate conțin specificații clare ale unor principii și obiective..., specifică cum vor fi accesate datele, ce date sunt accesibile și mai ales cui..., dar, din păcate, acestea sunt doar niște recomandări care nu determină eliminarea riscurilor, ci stabilirea unor direcții mai sigure în care să se desfășoare activitatea noastră.

Securitatea reprezintă o prioritate de business pentru 2012

Pe măsură ce tehnologia de cloud computing și mobilitatea schimbă mediul de business și modul în care definim ideea de birou, securitatea informațiilor din companii devine un element foarte important pentru îndeplinirea obiectivelor de business. Cercetările internaționale realizate recent de către firma HP confirmă această tendință și subliniază necesitatea ca toate companiile Instant-On să definească și să implementeze o strategie cuprinzătoare de administrare a riscurilor.

[Sursa: Devirusare.com]

Hai să mergem pe ideea de 10... adică zece așa-zise politici de securitate pentru utilizatori:

1. Tipuri de utilizatori (nu trebuie să uitați că pe același calculator pot “lucra” mai mulți utilizatori cu niveluri diferite de pregătire și mai ales de responsabilitate) – stabiliți o listă cu aceștia și atribuiți categorii administrator, respectiv utilizator standard funcție de situație

2. Utilizarea parolelor – schimbați regulat parolele (2-3 luni), nu folosiți aceeași parolă pentru mai multe locații, ridicați gradul de dificultate(caractere speciale, litere mari, spațiu, cifre)

3. Instalarea de aplicații – nu folosiți soft piratat (este doar o recomandare), verificați sursa softului ce urmează a fi instalat (chiar dacă folosiți soft piratat, aveți măcar grijă ca acesta să fi fost folosit/testat de alții înainte), atenție și la “fake software”

4. Actualizarea hardware și software – stabiliți o legătură între software-ul pe care-l instalați și hardware-ul existent, urmăriți și instalați up-date-urile de software, dacă se poate creați și un up-grade hardware pentru a răspunde mai bine cerințelor soft

5. Utilizarea antivirus – utilizarea unui antivirus nu presupune doar instalarea acestuia... înseamnă up-date-ul bazei de date, realizarea unei liste de zone de scanare, stabilirea și activarea unui program de scanare

6. Folosirea Internetului – alegerea unui browser care să răspundă mai bine cerințelor, stabilirea de reguli de utilizare, realizați up-date-urile de software





Este foarte important ca browser-ul pe care îl folosim să ofere un nivel cât mai ridicat de securitate. Nu doar viteza și facilitățile pe care extensiile ni le pot oferi sunt importante, ci și securitatea browser-ului. Vulnerabilitatea browser-ului poate porni fie de la browser-ul propriu-zis, fie de la plugin-urile respectiv extensiile instalate. Cu alte cuvinte, găurile de securitate ce pot fi exploatare își pot avea originea nu doar în browser-ul ca atare, ci și în plugin-uri.

7. Folosirea e-mailului – alegerea unui client care să răspundă mai bine cerințelor, stabilirea de reguli de utilizare, realizați update-urile de software

8. Criptarea datelor – protejați informația de pe calculator prin criptarea datelor, alegeți persoanele care să dețină cheia de criptare pentru decriptare.

9. Protecția fizică – folosiți elemente de protecție fizică pentru echipamente mobile (cablu de securitate, cu sau fără alarmă), folosiți măsuri de blocare furnizate de producător

10. Actualizarea politicii de securitate – chiar dacă este cea din urmă prezentată aici, după părerea mea, este și cea mai importantă... chiar dacă v-ați stabilit politici de securitate (mai ales în cazul firmelor) și nu le actualizați periodic (ex. noutăți de pe piață, lista utilizatorilor rămași și mai ales plecați din firmă – pentru ei, ștergerea drepturilor și conturilor), apar breșe de securitate.

Un studiu BitDefender scoate în evidență probleme de securitate la folosirea cardurilor bancare. Astfel, 57% dintre respondenți au declarat că au dezvăluit date confidențiale unor surse nesigure, iar 27% au recunoscut că nu au auzit de phishing.

Mijloace și metode de a asigura protecția

O să mergem tot pe ideea de 10... adică zece mijloace și metode de protecție pentru utilizatori:

1. AntiVirus – Avem nevoie de un antivirus (free sau achiziționat). De obicei au incluse și soluții AntiSpyware, AntiMalware, dar atenție la ce soft folosiți. Nu instalați programe pe care nu le cunoașteți. Dați o căutare pe Google pentru a afla mai multe informații. Există foarte multe programe antivirus pe Internet care sunt false (fake), dar care “arată/seamănă” cu unul real.





2. Software dedicat – De obicei alegerea unui program antivirus nu rezolvă toate problemele. Din această cauză trebuie să apelăm la soluții terțe. De exemplu, BitDefender USB Immunizer protejează dispozitivele periferice de stocare împotriva eventualelor infecții (tip autorun). Nu exagerați! Alegeți soluțiile de protecție mobile (care nu necesită instalare) pentru a elimina o eventuală încărcare fără rost a sistemului.

3. Firewall – Sistemul de operare are firewall-ul său, însă dacă considerați că acesta nu face față aveți două variante: una software – alegeți una dintre soluțiile de pe piață (ex. ZoneAlarm) și una hardware – mai scump, dar mult mai sigur (ex. Astaro Security Gateway).

4. Alegere Browser – cum mare parte din probleme vin din navigarea pe Internet, alegerea unui browser mi se pare un lucru foarte important (oricum, mai important mi se pare cum te comporți când navighezi pe Internet)... alegerea vă aparține.

5. Activarea filtrărilor și nivelurilor de securitate din browser – o utilizare mai sigură presupune și personalizarea setărilor privind conținutul, confidențialitatea și securitatea

6. Protecție email – cei care folosesc servicii web mail (Yahoo, GMail, Hotmail) sunt protejați direct de pe serverele respective (virusi, spam). Cei care au însă propriul lor server de mail (firmă, personal) trebuie asigurată o protecție suplimentară. Soluția aleasă ar trebui să conțină antispam, antivirus, control conținut, control imagini, criptare.

7. Criptarea datelor – dacă vorbim de pierderea sau furtul de date confidențiale, cea mai bună soluție de protecție este criptarea datelor. Windows 7 vine cu EFS (Encrypting File System) – sistem de fișiere cu criptare (BitLocker, Cipher)

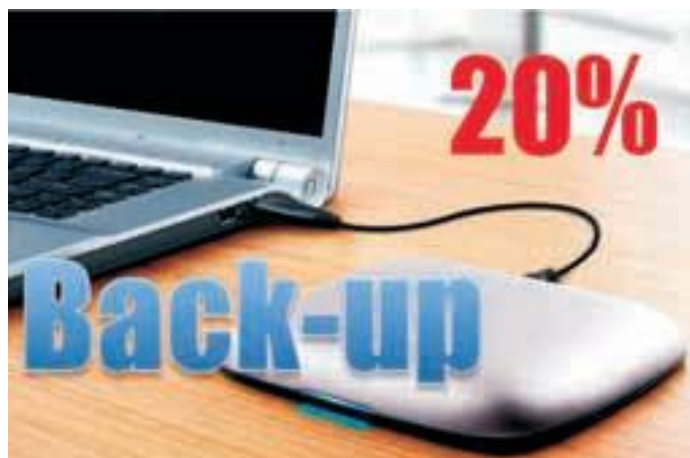
8. Audit Policy și Local Security Policy – Sistemul de operare ne poate furniza informații via Event Viewer despre modul de utilizare a sistemului (utilizatori, aplicații, eve-

nimente), informații pe care le putem utiliza pentru a preveni tîmpina sau rezolva probleme de securitate. De asemenea, chiar dacă este o zonă ceva mai sensibilă, o bună utilizare a Local Security Policy poate să rezolve câteva din problemele “nerezolvabile” – stabilirea de politici de securitate pe utilizatori, software, rețea.

9. Template-uri de securitate – Se pot folosi și template-uri de securitate via Microsoft Security Compliance Manager. O verificare a “calității” măsurilor de securitate luate o puteți obține cu ajutorul Action Center – Security.

10. Back-up date – am păstrat pentru final ceva foarte important... creați copii de siguranță. Copiile de siguranță trebuie să fie făcute pe suporturi de stocare externe, periodic, automat și trebuie să cuprindă cât mai multe date pe care le considerați importante.

Conform statisticilor, doar 20% dintre utilizatorii de echipamente de calcul își protejează prin back-up informațiile de pe suporturile de stocare, asta în condițiile în care, trebuie să recunoaștem, fișierele tale pot fi șterse accidental, corupte de către un virus sau pierdute definitiv atunci când vă cedează hard-ul etc.



Informare, educare, punerea în aplicare a măsurilor

Volumul de amenințări a crescut fantastic în ultima perioadă. De ceva timp amenințările se îndreaptă și către Apple Mac OS, datorită creșterii plajei de utilizatori, dar ponderea cea mai mare o are gama de sisteme de operare de la Microsoft. Investițiile au crescut pentru contracararea atacurilor și rezultatele nu se lasă așteptate... De exemplu, calculatoarele cu Windows 7 infectate de 5 ori mai rar decât cele cu Windows XP. Chiar dacă unele informații sunt îmbucurătoare, amenințările vor exista, dezvolta și diversifica permanent. Pentru aceasta, utilizatorii trebuie informați și educați în egală măsură. Un utilizator infectat este, pe lângă o problemă deschisă prietenilor, colegilor și mai ales a administratorilor de rețea, o sursă de propagare... Ceea ce am prezentat mai sus nu sunt decât vorbe în vânt dacă nu sunt și puse în aplicare... una din cele mai uzitate expresii este: “știam că ce trebuie să fac, dar nu credeam că o să mi se întâmple tocmai mie”. De multe ori ignorată, securitatea datelor unei companii intră în centrul atenției, în 95% din cazuri, abia după ce s-a consumat un eveniment ce a afectat în mod negativ activitatea companiei. Soluțiile profesionale de securizare a datelor costă, și în aceste condiții companiile de la noi își asumă riscul și preferă să angajeze un student pentru a alege o soluție de moment... Majoritatea companiilor românești nu sunt precaute și apelează la servicii de securitate IT numai după ce au fost afectate. Se vorbește chiar de un management al riscului, care să garanteze continuitatea afacerii. Succes în alegerea soluției optime pentru asigurarea siguranței și securității firmei dumneavoastră!

Nu uitați de propriii angajați. Aproape jumătate dintre angajații care își desfășoară activitatea într-o mare varietate de domenii au recunoscut ca au luat date cu ei când și-au schimbat locul de muncă, mergând de la documente și persoane de contact până la contracte și liste de prețuri. În general măsurile de securitate și regulile de conduită fie nu sunt luate în considerare, fie sunt ocolite. Conform Information Security Survey, utilizatorii chestionați au declarat că nu văd un obstacol în politicile de securitate IT ale companiilor la care lucrează, fiind capabili să obțină date din afara sediului companiei sau să iasă nestânjeniți pe ușă cu diverse suporturi de stocare – stick-uri USB, discuri optice inscripționate în companie, hard-discuri cu adaptor sau în rack USB etc. Dat fiind că atât de mulți angajați au recunoscut că au “păstrat” informații la schimbarea locului de muncă, 53% dintre aceștia suspectează că datele ce țin de proprietatea intelectuală a companiei sunt folosite de concurență. În jur de 42% dintre respondenți au apreciat că măsurile de securitate ale companiei lor sunt inexistente, insuficiente, nu sunt adaptate specificului activității sau sunt prea restrictive.

[Sursa: Datasecurity.ro].

