



## **Este compania dvs. securizată împotriva amenințărilor de securitate de pe Internet?**

Numeroși proprietari de întreprinderi mici și mijlocii (IMM) consideră că vulnerabilitatea corporațiilor mari la amenințările de securitate de pe Internet este mai accentuată decât cea a companiilor mici. În realitate însă, lucrurile stau altfel. De exemplu, conform datelor furnizate de organizația Internet Security Alliance, viermele distructiv Mydoom a afectat una din trei IMM-uri, însă doar una din șase companii mari.

Falsul sentiment de securitate afectează un număr semnificativ de IMM-uri, acestea considerând că nu sunt expuse riscurilor și, în consecință, neprotejându-și calculatoarele și rețelele împotriva amenințărilor de securitate precum software-uri spion, virușii, viermii, atacurile hackerilor și furtul de informații despre clienți. În plus, având deja de „jonglat” cu tot mai multe probleme, frecvent, întreprinzătorii plasează securitatea calculatoarelor în poziții inferioare ale listelor de priorități (dacă aceste listă există).

În consecință, conform studiilor firmei de cercetare AMI-Partners, aproape jumătate dintre IMM-uri nu și-au luat nici măcar măsuri elementare de securitate, cum ar fi instalarea de programe antivirus și antispyware.

### **Cauzele expunerii IMM-urilor la riscuri de securitate**

Expunerea mai mare ca niciodată a calculatoarelor, rețelelor și datelor IMM-urilor la riscuri de securitate se datorează mai multor factori.

Breșele în sistemele de securitate ale rețelelor de companie sunt mai dificil de realizat. În ultimii ani, securitatea rețelelor de companie a sporit în mod semnificativ datorită numărului tot mai mare al amenințărilor informatice provenite de pe Internet și al necesității conformării la reglementări noi, cum ar fi Basel II. În consecință, infractorii își îndreaptă tot mai insistent atenția spre țintele mai vulnerabile – IMM-urile.

Sistemele neprotejate sunt mai ușor de identificat. În prezent, numeroși hackeri dețin instrumente software care caută continuu pe Internet rețele și calculatoare neprotejate. Odată descoperite, calculatoarele neprotejate pot fi accesate și controlate de către hackeri, care le pot utiliza pentru a lansa atacuri asupra altor calculatoare sau rețele.

Amenințările de securitate sunt tot mai sofisticate și mai dăunătoare. Autorii de software-uri spion creează programe periculoase care sunt dificil de eliminat, suferă „mutații” continue și se răspândesc pe Internet în doar câteva minute. În același timp, apar tot mai multe amenințări combinate, îmbrăcând forme multiple și care sunt capabile să atace sistemele informatice pe mai multe planuri diferite. IMM-urile care nu adoptă soluții de securitate adecvate și actualizate pot fi cu ușurință afectate de amenințări de securitate de tipurile prezentate sau de alte tipuri.

Frecvent, amenințările de securitate sunt generate „din interior”. Prea adeseori, breșele în sistemele de securitate provin din interiorul companiilor și, de cele mai multe ori, sunt neintenționate. De exemplu, un angajat poate descărca, în necunoștință de cauză, software-uri spion atunci când joacă anumite jocuri online sau atunci când accesează anumite site-uri Web. Sistemele informatice ale IMM-urilor sunt mai vulnerabile la prejudiciile aduse involuntar de către angajați datorită absenței măsurilor de securitate interne tipice la companiile mari.

Impactul atacurilor la adresa securității informatice este mai mare. În numeroase cazuri, IMM-urile nu dispun de resursele financiare și tehnice utilizate de companiile mari pentru contracararea riscurilor de securitate. Dacă se lansează un atac de tipul DoS (blocare a serviciilor) împotriva unui IMM care furnizează servicii comerciale online, este puțin probabil ca veniturile pierdute să mai poată fi recuperate. În plus, efectele unui astfel de atac pot afecta grav relațiile cu clienți și reputația companiei.

## Care sunt soluțiile?

Din fericire, există numeroase soluții de protejare a unei companii împotriva amenințărilor de securitate de pe Internet. Primul pas este includerea problemei securizării accesului la Internet ca element fundamental în planul de priorități al companiei.

Nu este suficient ca acest plan să prevadă că securitatea informatică este o prioritate principală. Trebuie să existe un plan scris și detaliat dedicat securității, care să includă politici și proceduri specifice, precum și, în cazul companiilor cu mai mulți angajați, un plan conținând cerințele tehnologice. Dacă procedurile de securitate nu sunt sub formă scrisă, va fi ușor unor angajați să le conteste sau să le ignore.

De asemenea, mai există o serie de aspecte pe care IMM-urile nu ar trebui să le piardă din vedere:

- IMM-urile trebuie să evalueze procedurile și soluțiile de securitate implementate și să stabilească dacă acestea satisfac cerințele comerciale curente. Destul de frecvent, proprietarii IMM-urilor nu cunosc toate elementele incluse în soluțiile de securitate implementate. De exemplu, majoritatea routerelor pentru birouri la domiciliu și pentru rețele LAN de IMM-uri au încorporate tehnologii de tip *firewall*, care blochează accesarea de către intruși a calculatoarelor din rețea. Indiferent de situație, este important să se verifice caracteristicile și funcționalitatea elementelor de securitate implementate.
- Condiția minimă de securitate pentru calculator utilizat într-o companie este protejarea sa printr-un *firewall* hardware sau software și prin programe antivirus și antispyware. Unele soluții de securizare a accesului la Internet dedicate IMM-urilor combină toate cele trei elemente menționate anterior și, în plus, asigură protecție împotriva furtului de identitate, a *spam*-ului, a *phishing*-ului etc.
- Numeroase IMM-uri consideră că însăși luarea în considerație a aspectelor legate de securitatea informatică este o sarcină dificilă. Prin urmare, una dintre opțiuni este recurgerea la consultanță externă. Angajarea unui consultant în vederea efectuării unui audit de securitate al sistemelor și al rețelelor poate clarifica lista cerințelor strict necesare. De asemenea, soluțiile de securitate se pot stabili și de distribuitorii de echipamente de rețea și de furnizorii de tehnologii. O altă opțiune este recurgerea la servicii externe. Un furnizor de servicii administrate, cum ar fi furnizorul principal de servicii de telecomunicații, poate proiecta, implementa și întreține o soluție de securitate pentru rețea în schimbul unei taxe lunare relativ mici.
- Un alt aspect esențial este actualizarea regulată a soluțiilor de securitate adoptate de IMM-uri. În fiecare zi apar pe Internet noi amenințări de securitate. Dacă sistemele de securitate nu sunt actualizate rapid și în mod regulat, ele devin ineficiente împotriva virusilor, viermilor și software-urilor spion nou apărute. Din fericire, majoritatea software-urilor antivirus și a altor soluții de securitate se pot actualiza automat.

## Securitatea ca bază funcțională

Pentru succesul comercial al oricărui IMM, securitatea informatică reprezintă un element vital – mai ales dacă respectivul IMM se bazează, într-o măsură sau alta, pe accesul la Internet pentru desfășurarea proceselor comerciale. De asemenea, este important ca măsurile de securitate să nu fie excesive: este posibil ca un calculator să fie securizat împotriva oricărui tip de amenințare informatică, însă, din această cauză, să devină inutilizabil. IMM-urile trebuie să realizeze un echilibru adecvat între securitate și utilizabilitate.

Cu toate acestea, rețelele securizate asigură companiilor avantaje care depășesc contextul protecției împotriva amenințărilor informatice de pe Internet. Prin natura sa, o rețea securizată este o rețea robustă, iar o rețea robustă constituie o bază excelentă pentru implementarea tehnologiilor noi, cum ar fi comunicațiile bazate pe protocoale VoIP, care pot contribui în mod semnificativ la sporirea productivității și la reducerea costurilor operaționale.

În fine, atunci când o companie este securizată informatic, ea devine mai puternică, mai flexibilă și, cu certitudine, mai competitivă.

Pentru informații suplimentare, accesați site-ul Cisco dedicat IMM-urilor de la adresa [www.cisco.com/go/smb](http://www.cisco.com/go/smb) sau testați instrumentul Secure Business Advisor de la adresa [www.securebusinessadvisor.com](http://www.securebusinessadvisor.com).