



G Data press release 2012

Rezolutie privind securitatea IT pentru un an nou in siguranta

G Data ii chestioneaza pe utilizatori despre propria securitate IT pe perioada sezonului festiv



Bucuresti (Romania) 19.12.2012 – Sa renunti la fumat, sa faci curatenie in garaj sau sa slabesti 10 kg – sunt cateva decizii pe care le poti lua pentru perioada de sarbatori. Cu mai putin de doua saptamani ramase din acest an, e timpul sa te gandesti la obiectivele pentru 2013. G Data ii sfatuieste pe utilizatorii de Internet sa nu uite de propria securitate IT, deoarece infractorii cibernetici vor continua sa-i vizeze in anul ce urmeaza pentru a le fura datele cardurilor bancare, parolele si alte date personale. O securitate insuficienta ii ajuta pe atacatori si le usureaza munca. G Data face apel catre utilizatori sa-si creeze propriile rezolutii pentru 2013 si ofera 6 sfaturi pentru implementarea cu succes a acestora.

"Vulnerabilitatile programelor si computerele insuficient protejate sunt cai de acces ideale pentru infractori pentru a vana datele personale," explica Ralf Benz Müller, sef al G Data Security Labs. "Utilizatorii ar trebui sa-si securizeze propriile computere, sa foloseasca solutii de securitate eficiente si sa-si instaleze intotdeauna update-urile programelor instalate. In acest fel, atacatorilor le va fi foarte greu sa obtina date profitabile."

Sase rezolutii de securitate IT pentru utilizatorii de Internet

Update-uri instalate: Instalati toate Service Pack-urile disponibile, update-urile si patch-urile de securitate pentru sistemele de operare si pentru celelalte programe. Stergeti programele vechi si depasite care nu mai beneficiaza de suport de la furnizor si inlocuiti-le cu altele corespunzatoare.

Utilizati solutii de securitate: O solutie eficienta de securitate ar trebui sa fie parte integranta a echipamentului de baza al fiecarui utilizator de Internet si nu ar trebui sa includa doar protectie antivirus, ci si firewall, filtru anti-spam si protectie in timp real impotriva amenintarilor web. In plus, acestea trebuie sa fie actualizate cu regularitate.

Curatati hard-disk-ul: Utilizatorii ar trebui sa stearga toate datele care nu mai sunt necesare, la fel si fisierele duplicate, de pe hard-disk. Programe utilitare gratuite, de genul AntiTwin, ii ajuta pe utilizatori sa le identifice. De regula, aceste programe pot fi descarcate de pe site-urile revistelor de specialitate.

Schimbati parolele: Utilizatorii ar trebui sa-si schimbe cu regularitate parolele conturilor deschise pe magazine online, retele sociale sau alte portaluri online. O parola sigura trebuie sa contina numere aleatorii, caractere speciale, litere mici si majuscule. Cand alegeti o parola ar



trebuie să evitați termeni întâlniți în dicționare. În acest fel, spargerea parolelor de către hackeri devine mai dificilă.

Securizati dispozitivele mobile: Tabletele și smartphone-urile ar trebui echipate cu soluții de securitate fiabile, ce protejează împotriva programelor malware și împotriva furtului sau pierderii.

Backup de date: Prin backup se salvează toate datele personale, gen fotografii de familie sau videoclipuri, în caz de pierdere a datelor datorată unei infectări sau în cazul în care sistemul devine inoperant. În plus, o imagine a sistemului ne ajută să ne recuperăm întregul hard-disk împreună cu programele instalate. Suitele de securitate complete includ adesea și un modul de backup.

-###-