Comunicat de presa

Cel mai rau scenariu posibil: malware-ul de pe computerele companiilor!

White paper-ul de la G Data informeaza cum se pot proteja companiile impotriva atacurilor

Bucuresti (Romania), 24 Septembrie 2009 – Cum pot afecta virusii, troienii si viermii afacerile companiei? Care este scopul din spatele distributiei de malware? Cine dezvolta malware-ul si pentru ce profituri? Macinati de aceste intrebari si de altele similare nu sunt numai utilizatorii casnici de PC-uri. In special, expertii in securitate si administratorii de retele, responsabili cu buna functionare a retelei, sunt interesati de modul de operare a infractorilor astfel incat sa beneficieze de protectie optima impotriva atacurilor. White paper-ul G Data "Cum poate afecta malware-ul afacerile companiilor?" raspunde la aceste intrebari.

Infractorii online actioneaza rapid, nu lasa urme, iar tintele lor intra in moarte clinica. Indiferent daca sunt infectate doar cateva computere sau intreaga retea, consecintele pentru societatea in cauza sunt dezastruoase. Uneori, mai ales in cazul in care sunt implicate intreprinderile mici si mijlocii, rezultatul este o lupta pentru supravietuire economica.

Ralf Benzmuller, manager G Data Security Labs stie totul despre problema: "Odata ce un virus sau vierme este activ, compania are deja de suferit, o pierdere sau deteriorare, iar administratorul nu poate decat sa limiteze daunele. De aceea este vital sa asigure o protectie eficienta impotriva incercarilor infractorilor cibernetici de a introduce programe malware in retea. Pentru a oferi o aparare cat mai eficienta, administratorul de retea trebuie sa isi foloseasca avantajul de a cunoaste toate aceste dedesubturi, cine sunt dezvoltatorii de malware, care este scopul lor, precum si metodele utilizate pentru distributia de malware."

Economia subterana: salarii de milioane de dolari pentru hackeri
Motivatia hackerilor s-a schimbat foarte mult in ultimii ani: in timp ce inainte se putea discuta despre demonstratii intre colegii specialisti in computere, acum dezvoltatorii de virusi si viermi sunt motivati de castiguri pur financiare. Benzmuller stie ca ... "mai nou tranzactiile cu date si conturi furate sunt menite sa aduca o avere – cu care nici dealerii de droguri, nu mai pot tine pasul".

Deschizatorul de usi: stick-ul USB, operator de transport de virusi
Infectarea unei retele se poate face prin intermediul paginilor web, a e-mail-ului sau a serviciilor de file sharing si de mesagerie instant. De asemenea, stick-urile USB sau CD/DVD-urile pot contine programe cu potential de virusare. Utilizatorii de PC-uri au constientizat de-a lungul anilor ca exista un risc in a deschide fisierele atasate la e-mail, de

aceea infractorii au schimbat strategia: in loc de atasari de fisiere, infractorii au ales un alt mod de a transporta codurile malware, prin intermediul link-urilor catre site-uri aparent interesante. Un singur click pe un astfel de link este de multe ori suficient pentru a infecta computerul cu malware sau de a activa un botnet prin care sa poata prelua controlul asupra computerului.

Cinci sfaturi pentru o protectie eficientă a computerului

Deci, cum va puteti proteja impotriva unor astfel de atacuri nedorite? Expertul in securitate, Ralf Benzmuller, are urmatoarele sugestii:

Protectie antivirus
Protectia antivirus ar trebui sa fie instalata atat pe servere si clienti. Aceasta ar trebui sa verifice, de asemenea, si fluxul de date HTTP si, daca este necesar, datele de la sesiunile de chat (ICQ, IRC) pentru depistarea malware-ului. Dispozitivele portabile, cum ar fi notebook-urile si netbook-urile trebuie sa fie integrate in conceptul de securitate si protejate cu solutii independente de protectie impotriva virusilor si firewall-uri proprii.

Protectie antispam
Pentru ca e-mail-urile contin acum link-uri catre site-uri ilegale, mai degraba decat fisiere atasate, protectia antispam trebuie sa fie constituita dintr-o solutie independenta care sa actioneze simultan cu protectia antivirus impotriva malware-ului.

Firewall, detectarea si prevenirea intruziunilor
Datele provenite din traficul de retea pot fi folosite pentru a detecta si preveni atacurile in curs de desfasurare ale viermilor de pe Internet.

Management informat
Masurile de securitate trebuie sa fie acceptate si sustinute de catre angajati. Furnizarea periodica de informatii despre sursele de risc de pe Internet ii ajuta pe angajati sa se fereasca de pericole.

Solutiile de securitate G Data adresate corporatiilor: premiate pentru protectia antivirus oferita

Relativ recent, G Data a fost in masura sa demonstreze aptitudinile sale speciale in domeniul protectiei antivirus la nivel de corporatii. Din motive serioase, solutiile G Data adresate corporatiilor au primit, in luna mai, distinctia acordata marcilor de top intr-un test comparativ efectuat de catre bine cunoscutul laborator de cercetare din Austria, AV Comparitives.
Solutiile scalabile sunt prevazute cu o protectie imbatabila pentru retelele companiilor mici, mijlocii si mari. Conform cerintelor, administratorii de retele pot alege intre urmatoarele produse: AntiVirus Business 2010, AntiVirus Enterprise 2010, ClientSecurity Business 2010, ClientSecurity Enterprise 2010 sau MailSecurity 2010.

- ###-