



Comunicat de presă

Tendențele securității Internet – nu doar dintr-o perspectivă IT

Rapoartele Cisco și IronPort evidențiază amenințări noi și complexe

În efortul său de a lămuri mai explicit tendințele actuale privind amenințările de securitate informatică la nivel mondial, Cisco face public primul său raport privind starea globală a securității IT. În raport se evidențiază riscurile și problemele cu care se confruntă din ce în ce mai mult companiile, organizațiile guvernamentale și consumatorii și, de asemenea, se oferă sugestii de protejare împotriva acestora. La rândul său, IronPort – care face parte din Cisco din vara anului 2007 – a publicat propriul său raport, 2008 Internet Security Trends Report, care arată principalele tendințe actuale în domeniul securității IT și sugerează modalități de protejare împotriva noii și sofisticatei generații de amenințări Internet care se vor manifesta în viitorul apropiat.

În timp ce numeroase rapoarte de specialitate de final de an se concentrează asupra amenințărilor de securitate a conținutului (virusi, viermi, troieni, spam și phishing), raportul Cisco extinde discuția la un set de șapte categorii de management al riscurilor, dintre care unele depășesc problematica aspectelor izolate de securitate a conținutului. Categoriile avute în vedere se referă la vulnerabilitate, la aspectele fizice, la aspectele juridice, la încredere, la furtul de identitate, la aspectele legate de factorul uman și la aspectele geopolitice.

Rezultatele raportului subliniază faptul că amenințările de securitate și atacurile au devenit mai globale și mai sofisticate. Deoarece există tot mai multe dispozitive, aplicații și comunicații bazate pe IP, sporește și numărul de atacuri de securitate. Aceste tendințe scriu un capitol nou în istoria amenințărilor de securitate și a metodelor de atac.

Cu ani în urmă, virusii și viermii (Code Red, Nimda ș.a.) „scotoceau” sistemele de computere pentru provocarea de stricăciuni și obținerea de notorietate. Deoarece lucrul pe Internet și activitățile de e-commerce s-au intensificat, amenințările combinate (phishing facilitat de spam, atacuri din rețele zombi) au evoluat, urmărind furtul de bani și de informații personale. Această abordare de tipul „stealth-and-wealth” („disimulare și furt”) s-a extins deja la nivel mondial.

John Stewart, Chief Security Officer, Cisco, este de părere că securitatea informațiilor nu se mai rezumă doar la lupta împotriva virusilor sau a atacurilor spam. Frecvent, sunt implicați factori juridici, bazați pe identitate și geopolitici. Ca exemple, Stewart menționează furtul de identitate la firme de retail și un atac recent bazat pe tehnici DDoS (blocare distribuită a serviciilor) lansat, se pare, de hackeri motivați politic din Rusia și din Estonia. Atacul cibernetic, care, se pare, a fost cauzat de decizia autorităților estoniene de mutare a unui monument sovietic dintr-un parc, a închis numeroase site-uri Web ale administrației naționale.

„Infrafracționalitatea cibernetică evoluează vizibil, folosind adesea tehnici binecunoscute observate înainte numai sub formă electronică”, a declarat John Stewart. „Nu ne putem permite să considerăm amenințările de securitate IT drept dueluri singulare împotriva unor virusi sau a unor atacuri de tipul phishing; amenințările implică inginerii și tehnologii sociale, încredere și utilizare universală. În prezent, efortul de securizare a companiilor, a identităților personale și a informațiilor de importanță națională necesită un grad sporit de coordonare între entitățile care, în mod tradițional, nu au cooperat așa cum ar fi fost necesar: echipe de securitate IT, companii, structuri guvernamentale, poliție, consumatori și cetățeni. Toate acestea constituie ținte, însă, în același

timp, sunt și aliați. Eficiența securității la nivel național, de companie și personal va depinde de colaborarea și de comunicarea între toate aceste entități.”

Amatorismul a luat sfârșit

„2007 este un an de răscruce. Exact când structura software-urilor rău intenționate părea să se fi stabilizat, a avut loc o explozie de tehnici de atac noi, unele dintre ele într-atât de complexe – și, în mod evident, necreate de amatori – încât ne duc cu gândul la metode sofisticate de cercetare și de dezvoltare. Un timp, sistemele de controlare a aplicațiilor malware au funcționat. Însă, ca urmare a acestui succes, amenințările împotriva cărora asigurau protecția au fost forțate să evolueze. În anul 2007, numeroase amenințări informatice au suferit adaptări semnificative. Aplicațiile malware au început să acționeze disimulat, iar gradul lor de sofisticare a crescut,” a declarat Tom Gillis, Vice President of Marketing, IronPort

Informația este noua valută mondială

Mesajele spam, virușii și atacurile prin intermediul aplicațiilor malware sunt generatoare de costuri. Utilizatorul mediu petrece zilnic 5-10 minute pentru a administra mesajele spam. Eliminarea lor este estimată la 500 de USD per computer desktop. Încă și mai costisitoare sunt pierderile de date. Indiferent dacă sunt cauzate de acțiuni rău intenționate sau de erori accidentale, pierderile de date afectează imaginea, valoarea acțiunilor, fondurile comerciale și reputația companiilor. În prezent, la nivelul companiilor, cel mai semnificativ vector al pierderii de date este reprezentat de comunicațiile electronice și de datele în mișcare. Actualele firewall-uri și alte soluții de securizare a rețelelor nu includ capacități de prevenire a pierderilor de date care să securizeze datele în mișcare. Lipsesc o serie de elemente de control importante, cum ar fi scanarea conținutului, blocarea comunicațiilor care conțin date sensibile și criptarea. Se estimează că în ultimele 13 luni au fost expuse informații personale ale unui număr de circa 60 de milioane de persoane. De asemenea, se estimează că operațiile de securizare și scăderea productivității au generat, la nivel mondial, costuri de circa 20 de miliarde de dolari. Aproximativ 60% dintre datele companiilor sunt stocate pe PC-uri și laptopuri neprotejate. În plus, 48% dintre organizații nu au implementate politici de notificare a clienților cu date personale vulnerabile.

Privind în viitor: aplicațiile *malware* cu impact social

Aplicațiile malware moderne împrumută caracteristici ale comunicațiilor în rețea sociale și ale site-urilor Web colaborative asociate cu Web 2.0. Aplicațiile malware actuale (precum troianul „Storm”) sunt colaborative, adaptive, P2P (*peer-to-peer*) și inteligente. Ele „zboară sub plafonul de detecție radar”, rămânând nedetectate luni și chiar ani întregi în PC-urile de companie sau de la domiciliu. Noile versiuni de troieni și de aplicații malware vor fi din ce în ce mai mult direcționate și cu viabilitate redusă. Aceasta va spori și mai mult dificultatea detectării lor. Vechea atitudine de tipul „ceea ce nu văd nu-mi face rău” a devenit contraproductivă. Companiile sunt presate tot mai mult să asigure integritatea informațiilor sensibile – numere de carduri de credit, informații financiare sau planuri ale produselor noi. Autorii de aplicații malware creează rețele P2P sofisticate destinate colectării acestor date, iar detectarea și stoparea lor sporește continuu în dificultate. Echipele de securitate IT trebuie să acționeze în direcția monitorizării traficului de aplicații malware în rețele și a implementării de sisteme de securitate complexe care să includă tehnici avansate precum detectarea amenințărilor bazată pe rețea și controlul accesului în rețea.

Alte rezultate și statistici

Tendențele globale ale spam-ului și ale aplicațiilor malware pot fi caracterizate prin creșterea numărului de atacuri cu grad sporit de direcționare, de disimulare și de sofisticare. Iată câteva observații specifice:

- Volumul spam-ului s-a dublat, cifrându-se la peste 120 miliarde de mesaje spam zilnic. Aceasta înseamnă circa 20 de mesaje spam pe zi pentru fiecare individ de pe planetă.

Evaluările efectuate de IronPort arată că utilizatorii de la nivelul companiilor primesc zilnic între 100 și 1000 de mesaje spam.

- Spam-ul nu se mai concentrează atât de mult asupra vânzării de produse, ci a dezvoltării de rețele spam. Versiunile anterioare de atacuri spam urmăreau în principal vânzarea anumitor tipuri de produse (medicamente, împrumuturi ipotecare cu dobânzi mici etc.). Spam-ul actual include un număr sporit de linkuri către site-uri Web care distribuie aplicații malware. Frecvent, aceste aplicații malware sunt concepute în vederea extinderii rețelelor zombi care au generat inițial spam-ul. Pe parcursul anului 2007, Centrul de monitorizare a amenințărilor de la IronPort a măsurat o sporire cu 253% a „spam-ului rău intenționat” (spam conținând linkuri către site-uri cunoscute distribuitoare de aplicații malware). Aceasta este încă o dovadă a tendinței autorilor de aplicații malware de a combina tehnologiile de e-mail și cele Web pentru a propaga amenințări informatice.
- Virușii sunt mai puțin vizibili, însă tot mai numeroși. Autorii de viruși au evoluat de la apariția atacurilor cu distribuire în masă, cum ar fi „Netsky” și „Bagel”. În anul 2007, virușii au avut un grad sporit de polimorfism și, în general, au fost asociați cu proliferarea unor rețele zombi foarte sofisticate, precum „Feebs” și „Storm”. În doar o săptămână, Centrul de monitorizare a amenințărilor de la IronPort a detectat peste șase variante ale virusului Feebs, fiecare dintre acestea începând să se răspândească exponențial înainte de crearea semnăturilor.
- Durata tehnicilor specifice de atac s-a diminuat substanțial. În anii precedenți, autorii de spam utilizau tehnici tipice – de exemplu încorporarea de imagini – pe durata mai multor luni. Unele tehnici mai recente, precum spam-ul MP3, au durat numai trei zile. Însă există numeroase tipuri de astfel de atacuri așa-zise minore. În timp ce în anul 2006 principala tehnică nouă era spam-ul cu imagini încorporate, în 2007 au existat peste 20 de tipuri diferite de fișiere atașate utilizate în diverse tehnici de atac cu durată scurtă.

Pentru a accesa gratuit Cisco 2007 Annual Security Report:

http://www.cisco.com/web/about/security/cspo/docs/Cisco2007Annual_Security_Report.pdf

Pentru a accesa raportul IronPort: <http://www.ironport.com/securitytrends/>

Despre Cisco

Cisco, (NASDAQ: CSCO) este liderul mondial în comunicațiile Internet care transformă modul de conectare, de comunicare și de colaborare interpersonală. Informații despre Cisco se găsesc la adresa Web <http://www.cisco.com>. Pentru știri de ultimă oră, accesați site-ul Web de la adresa <http://newsroom.cisco.com>.

###

Cisco, sigla Cisco și Cisco Systems sunt mărci comerciale înregistrate sau mărci comerciale ale Cisco Systems, Inc. și/sau ale societăților afiliate din SUA și din alte câteva țări. Toate celelalte mărci menționate în acest document sunt proprietatea firmelor respective. Utilizarea termenului de partener nu implică o relație de parteneriat între Cisco și oricare altă companie. Acest document face parte din Informațiile Publice Cisco.