



COMUNICAT DE PRESĂ

Studiu global privind securitatea evidențiază: Creșterea numărului de apeluri privind problemele de securitate către centrele de asistență tehnică. Cheltuielile pentru securitate vor crește în anul 2007

Comportamentul riscant al lucrătorilor la distanță. Atitudinea față de IT determină două treimi dintre profesioniștii IT să mărească anul viitor investițiile pentru sporirea securității

Cisco a publicat astăzi rezultatele finale ale unui studiu global privind decidenții din domeniul IT. Studiul relevă un fenomen tratat cu gravitate de majoritatea acestora și anume că numărul de apeluri către centrele de asistență tehnică privind problemele de securitate este în creștere. Pentru protejarea angajaților care lucrează la distanță, majoritatea decidenților IT vor recurge anul viitor la sporirea investițiilor în securitate, două cincimi dintre aceștia anunțând investiții cu 10% mai mari în 2007.

Concluziile reprezintă rezultatul unei serii aprofundate de studii internaționale privind comportamentul online al angajaților la distanță. Efectuat în vara aceasta de către o firmă independentă de cercetare a pieței, studiul analizează răspunsurile oferite de peste 1000 de tele-angajați și 1000 de decidenți din domeniul IT din 10 țări: SUA, Marea Britanie, Franța, Germania, Italia, Japonia, China, India, Australia și Brazilia. Aceste rezultate recente evidențiază gravitatea aspectelor semnalate în studiul efectuat în luna octombrie. Cercetarea arată contradicțiile dintre conștientizarea de către teleoperatori a problemelor de securitate și comportamentul lor real, precum și percepția deconcertantă privind rolul profesioniștilor IT în controlarea utilizării dispozitivelor de la nivelul organizațiilor – laptop-uri, PDA-uri și telefoane inteligente.

În ansamblu, 38% dintre decidenții IT au raportat o creștere a numărului de apeluri către centrele de asistență tehnică privind problemele de securitate. Problematika acestor apeluri o constituie utilizatorii și dispozitivele lor, care cad pradă atacurilor din partea virusilor, înșelăciunii prin intermediul mesajelor *spam*, furtului de identitate și altor activități rău intenționate. În India, mai mult de jumătate dintre respondenții IT (55%) au raportat o creștere a numărului apelurilor de acest tip, iar majoritatea problemelor semnalate au fost legate de viruși (70%), de atacuri de înșelăciune activate prin mesaje de tip *spam* (61%) și de *spyware* (55%). *Spam*-ul și înșelăciunea au fost cel mai frecvent raportate – mai mult de jumătate (52%) dintre respondenții IT au declarat că aceste două amenințări au reprezentat un factor care a contribuit la creșterea numărului de apeluri referitoare la securitate.

În consecință, două treimi (67%) dintre respondenții IT au declarat că se așteaptă ca investițiile pentru soluții de securitate să crească anul viitor. Două cincimi (41%) se așteaptă ca investițiile să crească cu mai mult de 10%. Profesioniștii IT din China, India și

Brazilia – trei țări relativ nou-venite pe piața Internetului, însă caracterizate de economii cu ritmurile printre cele mai rapide de dezvoltare din lume – se situează pe primele locuri. Prezentăm în continuare procentajele de respondenți IT care intenționează să-și mărească investițiile în securitate în decursul anului viitor:

1. China:	90%; 52% - cu mai mult de 10%
2. India:	82%; 66% - cu mai mult de 10%
3. Brazilia:	81%; 65% - cu mai mult de 10%
4. SUA:	66%; 44% - cu mai mult de 10%
5. Italia:	66%; 34% - cu mai mult de 10%
6. Germania:	63%; 27% - cu mai mult de 10%
7. Marea Britanie:	61%; 33% - cu mai mult de 10%
8. Australia:	55%; 36% - cu mai mult de 10%
9. Japonia:	54%; 24% - cu mai mult de 10%
10. Franța:	51%; 29% - cu mai mult de 10%
Total mondial:	67%; 41% - cu mai mult de 10%

„Corelația dintre aceste rezultate și studiul efectuat luna trecută intitulat *„Faptele sunt mai grăitoare decât vorbele: În pofida comportamentului online riscant, numeroși teleoperatori se angajează în activități online riscante. Un studiu global arată o percepție deconcertantă asupra rolului profesioniștilor IT în securizarea informațiilor”* nu este o coincidență” a declarat Jeff Platon, Vice President of Security Solutions Marketing, Cisco Systems.

Studiul anterior arată că două treimi (67%) dintre angajații la distanță din întreaga lume au declarat că sunt conștienți de problemele de securitate care apar în activitățile de muncă online. Cu toate acestea, mulți dintre aceștia utilizează stațiile de lucru pentru a pirata rețelele wireless ale vecinilor, pentru a deschide e-mail-uri provenite de la surse necunoscute, pentru a descărca fișiere ale companiilor unde sunt angajați pe calculatoare personale și pentru a partaja dispozitive deținute de companii cu persoane din afara acestora. În plus, majoritatea tele-angajaților consideră că managerii au mai multă autoritate decât personalul IT în ceea ce privește controlarea modului de utilizare a dispozitivelor deținute de companii. Pe de altă parte, o parte dintre cei intervievați sunt de părere că monitorizarea activităților lor online nu ar trebui să privească pe nimeni.

„Aceste concluzii reprezintă o „chemare la luptă” a echipelor de securitate IT din organizații. Studiul arată cu claritate că recunoașterea de către utilizatori a existenței problemelor de securitate nu conduce întotdeauna la un comportament online sigur. Întrucât majoritatea utilizatorilor neglijează autoritatea personalului IT, nu există nici o motivație în favoarea colaborării cu aceste echipe, fapt care ar favoriza adoptarea unor bune practici de lucru online. Nu este deloc surprinzător că reacțiile personalului IT contribuie la sporirea numărului de apeluri către centrele de asistență tehnică și la creșterea cheltuielilor pentru securitate. Înțelegerea cauzelor acestor tendințe sporește necesitatea unor abordări progresive, bazate pe rentabilitate, în vederea protejării datelor și a angajaților companiilor” a adăugat Jeff Platon.

În opinia lui John. N. Stewart, Chief Security Officer, Cisco Systems, o astfel de abordare necesită un angajament ferm din partea conducătorilor companiilor în vederea dezvoltării unei „culturi bazate pe cunoașterea problemelor de securitate”. Stewart recomandă derularea unor programe educaționale dedicate diferitelor categorii de utilizatori și de culturi comerciale, crearea de posturi dedicate protejării securității informaționale la toate nivelurile de conducere și în toate departamentele, precum și oferirea de recompense

evidente utilizatorilor cu un comportament online adecvat. „Prezentarea câtorva experiențe negative la nivelul unei organizații poate reprezenta o metodă eficientă pentru sublinierea importanței securității”, a declarat John N. Stewart.

„Tehnologia este un element important pentru securitate, însă nu constituie un panaceu universal. Securitatea este mai înainte de toate un exercițiu uman, reprezentând un aspect interpersonal care presupune comunicare și un angajament ferm în favoarea educației, a instruirii și a cunoașterii. Îmbinați relațiile puternice IT–utilizator cu soluțiile tehnologice și imaginea IT se va transforma în mod firesc într-o prezență strategică, cu rol consultativ, care va impulsiona formarea unei culturi organizaționale bazate pe conștientizarea importanței securității. Atunci când se va realiza acest lucru, decidenții vor acorda o atenție maximă implementării soluțiilor de securitate și, în același timp, vor preveni riscurile de subminare a productivității. Altfel spus, decidenții au puterea să ajute la bunul mers al companiilor, a spus John N. Stewart

Pentru informații suplimentare despre studiu, rezultate globale și concluzii specifice pentru fiecare dintre cele 10 țări, consultați studiul tehnic publicat pe pagina Web de la adresa: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_papers_list.html

Despre Cisco Systems

Cisco (NASDAQ: CSCO) este liderul mondial în comunicațiile Internet. Știrile și informațiile Cisco sunt disponibile la adresa Web <http://www.cisco.com>. Pentru știri de ultimă oră, accesați pagina Web de la adresa <http://newsroom.cisco.com>.

###

Cisco, sigla Cisco, Cisco Systems și sigla Cisco Systems sunt mărci înregistrate 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.