



Comunicat de presă

Studiul Cisco privind operatorii la distanță demonstrează necesitatea sporirii eforturilor de securizare

Studiul global evidențiază evoluția disimulată a amenințărilor IT drept cauză potențială a diminuării disciplinei în comunicațiile online și necesitatea sporită a întreprinderii de acțiuni în domeniul IT

Cisco prezintă rezultatele studiului anual privind gradul de informare despre problemele de securitate și modelele comportamentale în comunicațiile online ale operatorilor la distanță. Acesta evidențiază cauzele vulnerabilizării accidentale a informațiilor proprii și a celor aparținând companiilor pentru care lucrează, arată necesitatea furnizării de recomandări echipelor de IT privind protejarea companiilor împotriva amenințărilor informatice și maximizarea avantajelor comerciale generate de forța de muncă distribuită și mobilă.

Realizat de InsightExpress, o firmă de cercetare a pieței cu sediul în SUA, studiul cuprinde informații obținute de la peste 2.000 de operatori la distanță și profesioniști IT din companii cu domenii de activitate diverse din 10 țări: Statele Unite, Marea Britanie, Franța, Germania, Italia, Japonia, China, India, Australia și Brazilia. Aceste 10 țări au fost alese deoarece reprezintă o diversitate de culturi sociale și comerciale, de economii stabile și în formare și de zone cu grade diferite de adoptare a Internetului.

Semnificația studiului sporește în importanță datorită creșterii numărului de operatori la distanță în întreaga lume. Conform raportului Gartner pentru anul 2007, „la nivel mondial, între 2007 și 2011, numărul de teleoperatori din cadrul companiilor care petrec cel puțin o zi pe lună lucrând la domiciliu va cunoaște o rată anuală de creștere de 4,3%. În aceeași perioadă, tot la nivel mondial, numărul de teleoperatori din cadrul companiilor care petrec cel puțin o zi pe săptămână lucrând la domiciliu va cunoaște o rată anuală de creștere de 4,4%. La sfârșitul anului 2011, această populație se va cifra la 46,6 milioane de persoane.”¹

„Accesul la distanță și forța de muncă distribuită vor deveni ceva obișnuit. Acestea asigură avantaje concurențiale și eficiență operațională sporită. Companiile au posibilitatea să beneficieze de creșteri ale productivității și să prevină riscurile de securitate care le pot afecta operaționalitatea. Acest studiu oferă informații și recomandări pentru înțelegerea și minimizarea riscurilor, deoarece, în prezent, companiile permit angajaților să lucreze și în alte locuri decât birourile tradiționale. Studiul explorează aspectele comportamentale ale operatorilor la distanță și furnizează informații valoroase despre viziunea acestora asupra securității,” a declarat John N. Stewart, Chief Security Officer, Cisco)

Un fals sentiment de siguranță?

Una dintre observațiile-cheie este faptul că operatorii la distanță nu consideră ca prioritară vigilența la lucrul online. Deși majoritatea consideră că sunt mai vulnerabili atunci când lucrează în afara birourilor, percepția lor asupra amenințărilor de securitate este deficitară. Pe parcursul unui singur an, numărul operatorilor la distanță care consideră că Internetul este mai sigur a crescut cu 8% (de la 48% la 56%). Această tendință prevalează în Brazilia (71%), India (68%) și China (64%) – trei

dintre țările cu economiile cele mai dinamice și a căror forță de muncă depinde tot mai mult de Internet și de rețelele de companie.

Conform studiului, respondenții IT consideră că angajații la distanță devin tot mai indisciplinați în comportamentul online. Mai mult de jumătate (55%) consideră că operatorii la distanță acordă mai puțină importanță informațiilor despre amenințările de securitate, iar 11% cred că situația este mai bună din acest punct de vedere comparativ cu anul precedent. Schimbarea de percepție se poate datora evoluției peisajului amenințărilor – de la atacuri vădite la atacuri disimulate. Conform raportului pentru 2007 privind infracționalitatea și securitatea IT a Computer Security Institute, numărul atacurilor motivate financiar l-a depășit pe cel al atacurilor rău intenționate tradiționale (cu viruși, viermi și spyware) și, pentru prima oară în cei 12 ani de când se efectuează această monitorizare, pierderile medii anuale datorate atacurilor cu scop de fraudare le-au depășite pe cele cauzate de aplicații malware. Deși amenințările actuale au un grad sporit de pericolozitate deoarece sabotează nu numai informațiile companiilor, ci și datele personale, natura lor invizibilă creează angajaților un fals sentiment de siguranță, fapt care poate cauza diminuarea disciplinei în comportamentul online, mai ales când acesta se efectuează la distanță.

„Atunci când lucrează la domiciliu, angajații au tendința să „lase garda jos” mai mult decât atunci când sunt la birou; de aceea, aderarea la politici de securitate nu pare întotdeauna, intuitiv, la fel de aplicabilă și de necesară în cadrul privat”, a continuat Stewart. „Diminuarea diferențelor dintre munca la birou și cea la domiciliu și dintre „viața în cadrul companiei” și cea personală devine o provocare tot mai serioasă pentru companiile care caută să capitalizeze avantajele de productivitate ale forței de muncă la distanță.”

Iată o serie de rezultate-cheie ale studiului și cauze ale comportamentului riscant:

- **Accesarea e-mailurilor și a fișierelor atașate provenite de la surse necunoscute sau suspecte:** Deși este unul dintre riscurile vechi de securitate, numeroși operatori la distanță recunosc că deschid în continuare e-mailuri și fișiere atașate suspecte în pofida potențialului acestora de a declanșa atacuri cu aplicații malware. Cele mai multe atacuri provin din China (62%). Însă, indiscutabil, mult mai neliniștitoare este tendința în creștere manifestată în Marea Britanie (48%), în Japonia (42%), în Australia (34%) și în SUA (27%). De exemplu, în Japonia, 14% dintre respondenți au recunoscut că accesează e-mailurile și fișierele atașate din surse necunoscute sau suspecte.
- **Utilizarea computerelor și a dispozitivelor de la birou în scop personal:** O creștere anuală cu 3% arată că tot mai mulți operatori la distanță folosesc echipamentele companiilor în scop personal – efectuarea de cumpărături pe Internet, descărcarea de melodii și accesarea site-urilor de conectivitate socială. Această tendință se manifestă în 8 dintre cele 10 țări, creșterea cea mai semnificativă fiind cea din Franța (de la 27% la 50%). În Brazilia, această tendință a atins 16%, în pofida creșterii numărului de respondenți care consideră că acesta este un comportament inacceptabil (de la 37% la 52%).
Motivații oferite: „Conducerea companiei nu are nimic împotriva acestei practici.”, „Sunt singur și dispun de timp liber.”, „Șeful meu nu este în preajmă.”, „Departamentul de IT mă va ajuta dacă se întâmplă ceva.”
- **Permiterea împrumutării de către persoane din afara companiei a unor computere și dispozitive de la birou pentru utilizare în scopuri personale:** Deoarece tot mai mulți angajați lucrează la domiciliu, crește probabilitatea partajării dispozitivelor aflate în proprietatea companiei cu alte persoane (de exemplu membri ai familiei sau colegi de cameră) care nu au cunoștințe suficiente în domeniul IT sau care nu respectă politicile de securitate ale companiei. Această tendință este în creștere. Deși cea mai mare rată de „partajare a dispozitivelor” este în China (39%), creșteri semnificative de la un an la altul s-au înregistrat și în Marea Britanie (de la 7% în 2006 la 22% în 2007) și în Franța (de la 15% în 2006 la 26% în 2007).
Motivații oferite: „Nu văd nimic rău în aceasta.”, „Conducerea companiei nu are nimic împotriva acestei practici.”, „Nu cred că, procedând astfel, sporesc riscurile de securitate.”, „Și ceilalți colegi de muncă procedează la fel.”

- **Piratarea conexiunilor wireless la Internet ale vecinilor:** La nivel global, 12% dintre operatorii la distanță recunosc faptul că accesează conexiunile wireless ale vecinilor. Cele mai rapide rate de creștere anuală se înregistrează în Japonia (de la 6% la 18%) și în Franța (de la 5% la 15%). Cifre semnificative se înregistrează și în China (de la 19% la 26%) și în Marea Britanie (de la 6% la 11%).
Motivații oferite: „Am procedat astfel pentru că eram constrâns.” „E mai convenabil astfel.” „Nu știu exact dacă utilizez propria mea conexiune wireless sau cea a altcuiva.” „Vecinul meu nu știe, așa că totul este în regulă.”
- **Accesarea fișierelor de lucru cu dispozitive personale, neprotejate IT:** Accesarea rețelelor de companie și a fișierelor de lucru cu dispozitive neprotejate IT sporește riscurile la care sunt expuse companiile, informațiile operaționale și angajații. Deoarece numărul de operatori la distanță este în creștere, studiul arată o creștere anuală semnificativă a acestui comportament (de la 45% în 2006 la 49% în 2007). Tendința este răspândită în numeroase țări, mai ales în China (76%), SUA (55%), Brazilia (52%) și Franța (48%).
Motivații oferite: „Aceste dispozitive sunt securizate cu programe antivirus și alte software-uri de securizare a conținutului.” „Folosesc în mod regulat aceste dispozitive pentru a-mi accesa rețeaua.” „Cei de la departamentul de IT mi-au spus că este în regulă dacă procedez astfel.”

Recomandări strategice pentru protejarea forței de muncă distribuite în continuă creștere

John N. Stewart consideră că, acum mai mult ca oricând, este imperios necesar ca departamentele de IT să reevalueze percepția angajaților asupra activităților online și modalitățile de influențare proactivă a securității IT la nivelul companiilor. Frecvent, echipele IT abordează securitatea exclusiv dintr-o perspectivă tehnologică, însă necesitatea informării, educării și comunicării proactive și susținute privind securitatea este la fel de fundamentală ca și achiziționarea unui firewall. Împărtășirea acestor acțiuni consultative cu angajații reprezintă o oportunitate-cheie pentru echipele IT de a remodela perspectiva utilizatorilor asupra comunicațiilor online și a maximiza rentabilitatea investițiilor în tehnologii. O atare abordare asigură baza reconsiderării percepției asupra domeniului IT – de la un generator de costuri la un facilitator al proceselor comerciale. Abordarea multiculturală a studiului evidențiază necesitatea ca liderii din domeniul securității IT să aplice strategii „localizate” și mai direcționate pentru diversele regiuni ale globului.

„Rezultatele acestui studiu întăresc necesitatea de a corobora informarea, educarea și comunicarea la nivelul echipelor, al structurilor de conducere și al angajaților”, a declarat Stewart. „Modalitățile de comunicare și de educare a angajaților în ceea ce privește practicile de securitate esențiale vor fi diferite în Japonia și în SUA, de exemplu. La fel, nu vor fi aceleași în China și în Franța. Informarea și educarea în domeniul securității IT necesită înțelegerea culturii publicului căreia i se adresează. Sunt necesare relaționarea și câștigarea încrederii. Încrederea atrage după sine respect și cooperare.

„Acest studiu subliniază faptul că administrarea securității are mai multe componente: o componentă legată de tehnologii și o componentă de informare, educare și comunicare”, a adăugat Stewart. „Este vorba mai mult de o provocare socială decât de una tehnică. Și, datorită acestui lucru, domeniul IT trebuie să părăsească biroul tradițional și să se implice mai proactiv și mai consultativ în baza sa de utilizatori. Mai pe scurt, este momentul ca domeniul IT să devină mai strategic ca oricând.”

¹ Gartner, Inc., „Dataquest Insight: Teleworking, The Quiet Revolution (actualizare 2007)” de Caroline Jones, 14 mai 2007

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.