



Uno studio Cisco sui lavoratori in remoto rivela la necessità di una maggiore attenzione alla sicurezza. 3 professionisti IT su 5 hanno in programma di aumentare le spese per la protezione dai rischi informatici nel 2008

Una ricerca effettuata a livello globale analizza le conseguenze della leggerezza con cui i lavoratori in mobilità approcciano la sicurezza. La poca visibilità delle nuove minacce informatiche riduce la percezione dei rischi e il rispetto delle norme di comportamento per una navigazione sicura.

Milano, 26 marzo 2008 - Cisco ha annunciato i risultati della **seconda edizione** del suo studio annuale sui lavoratori in remoto, che analizza i loro comportamenti e le loro percezioni in materia di sicurezza. Dallo studio emerge che essi possono accrescere, senza rendersene conto, i rischi per sé stessi e per l'azienda, con serie implicazioni per i reparti IT; per fare fronte al fenomeno, infatti, ben tre professionisti IT su cinque fra gli intervistati hanno dichiarato di avere in programma aumenti di spesa per il 2008.

I dati emersi hanno spinto gli esperti di sicurezza Cisco a formulare raccomandazioni rivolte ai professionisti IT, relative ai metodi per proteggere le imprese dalle minacce e allo stesso tempo massimizzare i vantaggi per il business che derivano dall'avere una forza lavoro distribuita e mobile.

Commissionato da Cisco e condotta dalla società di ricerca indipendente Insight Express, lo studio ha coinvolto oltre 2.000 utenti professionali in mobilità e professionisti informatici di diversi settori merceologici, in 10 paesi: Stati Uniti, Regno Unito, Francia, Germania, Italia, Giappone, Cina, India, Australia, Brasile. Questi paesi sono stati scelti perché nell'insieme rappresentano culture aziendali e società molto diverse, includono sia economie emergenti sia economie mature ed hanno diversi livelli di adozione del web.

Una falsa tranquillità?

Uno dei dati più interessanti emersi dalla ricerca è che i lavoratori in remoto oggi **percepiscono meno l'importanza di controllare il proprio comportamento online**. Anche se la maggior parte di essi ritiene che si corrano più rischi lavorando fuori dall'ufficio che al suo interno, la percezione delle minacce informatiche si sta indebolendo. Il numero di lavoratori convinto che Internet sia diventata più sicura rispetto all'anno precedente è cresciuto dell'8% - passando dal 48% del 2006 all'oltre 56% del 2007. Questo trend è molto forte in Brasile (71%), India (68%) e Cina (64%): tre delle economie mondiali che crescono più rapidamente, in cui la forza lavoro dipende sempre più dal web e dalle reti aziendali.

I professionisti IT coinvolti nello studio ritengono che gli impiegati che lavorano a distanza stiano diventando sempre meno disciplinati nel loro comportamento online. Più della metà (il 55%) pensa che stiano diventando meno consapevoli dei rischi di sicurezza: una percentuale più alta di 11 punti rispetto a quella registrata l'anno precedente.

Questo fenomeno può essere il risultato dell'evoluzione delle minacce informatiche, che a differenza di prima oggi agiscono in modo poco visibile. Secondo il rapporto 2007 sul crimine informatico e la sicurezza del Computer Security Institute, il numero di attacchi di natura finanziaria ha superato quello dei tradizionali attacchi malware, e per la prima volta la perdita media annuale dovuta da attacchi fraudolenti ha superato quella generata dai danni malware. Anche se le odierne minacce sono più pericolose, perché mirano all'identità delle persone e ai dati sensibili delle aziende, la loro natura "invisibile" crea un falso senso di tranquillità fra i dipendenti, che può causare una minore disciplina nel comportamento online, in particolar modo quando si lavora a distanza.

“Quando lavorano da casa, le persone tendono ad abbassare la guardia molto più che in ufficio, dal momento che adeguarsi alle policy di sicurezza non sembra così semplice o così necessario finché si è fra le mura domestiche” spiega **John N. Stewart**, Chief Security Officer di Cisco Systems.

“Lo sfumarsi della distinzione tra ambiente lavorativo e domestico e fra la vita aziendale e personale rappresenta una sfida sempre più importante per le aziende che desiderano capitalizzare i vantaggi in produttività portati dall'aver lavoratori in remoto”.

I comportamenti a rischio: alcuni dati

Che si tratti di lavoratori dei paesi emergenti o meno, i comportamenti a rischio sono diffusi e, in molti casi, in crescita rispetto all'anno precedente. Lo studio ha indagato nel dettaglio i problemi che possono derivare dall'utilizzo poco sicuro dei dispositivi aziendali da parte dei lavoratori in mobilità, e le principali evidenze sono le seguenti.

Apertura di e-mail e allegati provenienti da fonti sconosciute o sospette: anche se è uno dei rischi di sicurezza noto da più tempo, molti lavoratori ammettono di aprire ancora e-mail sospette e allegati nonostante il rischio potenziale di dare il via a un attacco malware. La Cina è il paese che meno rispetta questa norma di sicurezza (62%), ma è ancora più preoccupante la tendenza a non curarsi di questo aspetto in paesi che hanno ormai adottato in modo esteso il web, quali il Regno Unito (48%), il Giappone (42%), l'Australia (34%) e gli USA (27%). **In Italia il 33% dei lavoratori apre le e-mail ma non gli allegati; un 4% dichiara di fare entrambe le cose.**

Utilizzo del computer e altri dispositivi di lavoro per motivi personali: una crescita anno su anno del 3% mostra che sempre più lavoratori in remoto usano gli strumenti aziendali a scopo personale, come per fare shopping online, scaricare musica, visitare siti di social networking. Questo trend è presente in otto paesi sui dieci presi in esame, e la crescita più evidente anno su anno si è avuta in Francia (dal 27% al 50% dei lavoratori). In Brasile è stato registrato un aumento di 18 punti percentuali, nonostante molti degli intervistati si siano dichiarati d'accordo sul fatto che questo è un comportamento non accettabile (la percentuale è passata dal 37% al 52%). **In Italia la crescita anno su anno è stata del 9% (da 21% a 30%).**

Permettere a persone esterne all'azienda di usare i pc e gli altri dispositivi a scopo personale: quanto più i dipendenti lavorano da casa, tanto più aumenta la possibilità che condividano gli strumenti informatici aziendali con non dipendenti (familiari, coinquilini) che non hanno adeguate conoscenze IT e non sono vincolati a policy di sicurezza aziendali. Questo trend è in crescita. Mentre in Cina si registra il maggior livello di "condivisione" (il 39% dei lavoratori lo fa), il Regno Unito e la Francia registrano la crescita maggiore del fenomeno anno su anno (rispettivamente passando dal 7% del 2006 al 22% del 2007 e dal 15% al 26%). **In Italia nel 2007 il 31% dei dipendenti che lavorano in remoto hanno avuto questo comportamento, contro il 19% registrato l'anno precedente.**

Usare abusivamente connessioni internet wireless presenti nelle vicinanze: globalmente, il 12% dei lavoratori mobili ammettono di accedere alle reti wireless dei vicini. La percentuale si è triplicata anno su anno in Giappone (dal 6 al 18%) ed è aumentata del 10% in Francia (dal 5 al 15%). Si sono registrati aumenti significativi anche in Cina, dove i lavoratori che si comportano in questo modo sono passati dal 19% del 2006 al 26% del 2007, e nel Regno Unito (dal 6 all'11%). **In Italia** la percentuale è salita del 6%, passando dal 12% del 2006 al 18% del 2007

Utilizzare file aziendali con dispositivi personali, senza adeguata protezione IT: accedere alle reti aziendali e ai file con *device* non protetti dal team IT è un rischio per l'impresa, per le sue informazioni e per i dipendenti. Con la crescita del numero dei lavoratori in remoto, lo studio ha evidenziato una maggiore portata (dal 45% al 49%) di questo comportamento. E' ampiamente diffuso in vari paesi, quali la Cina (76%), gli USA (55%), il Brasile (52%) e la Francia (48%). **Anche in Italia** il comportamento è molto diffuso: il 49% degli intervistati ha dichiarato di averlo fatto nel 2007, contro il 45% dell'anno precedente.

Le implicazioni economiche dei comportamenti a rischio

Nel corso della ricerca, il 62% del personale IT intervistato ha dichiarato che aumenterà la spesa relativa alla sicurezza per il 2008; di questi, più della metà (pari al 37%) ritiene che i suoi investimenti in security saranno maggiori di più del 10% rispetto al budget previsto l'anno precedente.

Analizzando i risultati a livello dei singoli paesi, emerge che nelle economie emergenti e in crescita, relativamente "nuove" alla diffusione di Internet e delle reti aziendali su IP, sono presenti il maggior numero di decisori IT che hanno deciso di aumentare le spese informatiche in generale nel 2008, e che ritengono di investire un budget superiore di più del 10% rispetto a quello allocato nel 2007.

Il motivo? Secondo Stewart ciò avviene perché un gran numero degli impiegati che utilizzano la rete in Cina, India, e Brasile non sono stati colpiti da Code Red, NIMDA, e gli altri famigerati attacchi malware in modo così pervasivo come è avvenuto nei paesi che hanno economie orientate al mondo consumer e dipendenti da Internet, come Stati Uniti, Regno Unito, Francia, Germania, e Giappone, ed hanno quindi meno esperienza dei danni che le minacce possono causare. Tuttavia, oggi questi Paesi rappresentano tre delle economie a più rapida crescita, e la loro dipendenza da Internet e dalle reti aziendali sta accelerando. La ricerca mostra che il comportamento rischioso dei lavoratori in remoto in queste tre nazioni, come l'apertura di e-mail di dubbia provenienza, lo sfruttamento delle connessioni wireless dei vicini di casa, o l'utilizzo condiviso dei dispositivi aziendali con altre persone al di fuori dell'azienda, è molto più diffuso di altre zone che hanno alle spalle una maggiore esperienza nell'uso di Internet per scopi aziendali.

Anche se Cina, India, e Brasile hanno la più alta percentuale di stima di crescita della spesa per la sicurezza, la tendenza non riguarda solamente i paesi emergenti. Più della metà degli intervistati in 8 nazioni su 10 sta progettando di aumentare la spesa in sicurezza entro quest'anno:

- **India:** 83% (60 % intende aumentare la spesa di più del 10%)
- **Cina:** 83% (58 % intende aumentare la spesa di più del 10%)
- **Brasile:** 68% (56 % intende aumentare la spesa di più del 10%)
- **Germania:** 61% (31 % intende aumentare la spesa di più del 10%)
- **Italia:** **60% (35 % intende aumentare la spesa di più del 10%)**
- **Regno Unito:** 58% (29 % intende aumentare la spesa di più del 10%)
- **Australia:** 55% (30% intende aumentare la spesa di più del 10%)
- **Stati Uniti:** 53% (27 % intende aumentare la spesa di più del 10%)

- **Francia:** 49% (22 % intende aumentare la spesa di più del 10%)
- **Giappone:** 24% (15% intende aumentare la spesa di più del 10%)

§ **In media: 62 % (37 % intende aumentare la spesa di più del 10%)**

In prospettiva: raccomandazioni per proteggere una forza lavoro distribuita e individuare “buoni” e “cattivi” investimenti in sicurezza.

Secondo John N. Stewart, oggi più che mai è imperativo che i reparti IT si impegnino per modificare la percezione che hanno di loro i dipendenti e per affermare l’influenza che possono esercitare in modo proattivo riguardo alla sicurezza aziendale. L’IT spesso pensa alla sicurezza solamente da un punto di vista tecnologico, ma generare consapevolezza sui temi della security, fare cultura in merito, comunicare in modo proattivo e sostenuto è tanto importante quanto la messa in opera di tecnologia. Diffondere questo impegno collettivo alla sicurezza fra i dipendenti è una grande opportunità per acquisire una nuova immagine agli occhi degli utenti e per massimizzare il ritorno degli investimenti in tecnologia.

“La ricerca evidenzia il fatto che gestire la sicurezza aziendale è in parte una questione di tecnologia, in parte di processo, di consapevolezza, di educazione e comunicazione” ha dichiarato Stewart. “E’ spesso più una sfida legata al fattore umano che una sfida tecnica. E per questo, l’IT ha il dovere di emergere dal suo ruolo di back office a un ruolo più proattivo, impegnato e di consulenza verso gli utenti. In poche parole, è il momento che l’IT diventi più che mai un fattore strategico”.

La sicurezza è un’esigenza aziendale molto concreta, e Stewart afferma che la ricerca fornisce una visione globale per l’IT al fine di adottare un approccio pratico per proteggere i propri dipendenti e le imprese, soprattutto nel momento in cui diventano più localmente distribuite. Proprio come sono necessari i budget per l’IT, così lo è la spesa per la sicurezza. Ciò che è importante, ha dichiarato, è comprendere la differenza tra una spesa che è considerata “accettabile” e una “irragionevole”. L’obiettivo è evitare che la spesa per la sicurezza sia reattiva, per così dire a danno avvenuto.

“Le aziende hanno bisogno di firewall, reti private virtuali, e di tecnologie per la protezione dei dati”, aggiunge Stewart. “La sfida sta nel ridurre al minimo le altre spese che avrebbero potuto essere evitate attraverso un’intensa attività di educazione dei dipendenti, come ad esempio la gestione di attacchi malware e furto di dati. Che la conoscenza sia lo strumento di protezione più efficace non è una novità; la novità è il modo in cui l’IT è a capo di persone, processi e tecnologia per proteggere le imprese nel modo più efficace. Accresce la consapevolezza degli impiegati attraverso una formazione continua riduce le minacce, gli attacchi, e le costose conseguenze che solitamente portano con sé.”

Cisco

Cisco (NASDAQ:CSCO) è leader mondiale nella fornitura di soluzioni di rete che trasformano il modo con cui le persone comunicano e collaborano. del Notizie e informazioni relative alla società ed ai prodotti sono disponibili all’indirizzo <http://www.cisco.com/>

<BLOCKED::<http://www.cisco.com/>> Le apparecchiature di Cisco Systems sono fornite in Europa da Cisco Systems International BV, una consociata interamente controllata da Cisco Systems, Inc.

###

Ufficio Stampa
Cisco Italy
Cristina Marcolin
Susanna Ferretti

Tel: 039/62951

email: pressit@external.cisco.com <<mailto:pressit@external.cisco.com>>