PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 9 - numero 1622 di lunedì 08 gennaio 2007

Telelavoratori e sicurezza aziendale

Percezioni e comportamenti dei telelavoratori: fattori chiave per la sicurezza aziendale. I dati di una ricerca.

Un recente studio commissionato da Cisco e realizzato a livello globale da Insight Express - importante società di ricerca indipendente - ha mostrato che sebbene i telelavoratori affermino di essere a conoscenza delle problematiche di sicurezza, il loro comportamento - che include la condivisione dei computer aziendali con persone al di fuori dell'ambito lavorativo, l'apertura di e-mail di dubbia provenienza e l'utilizzo non autorizzato di reti wireless altrui - lascia supporre il contrario, ovvero che non sia del tutto noto quale sia potenzialmente l'impatto negativo dei loro comportamenti sulla sicurezza aziendale.

Lo rende noto CLUSIT (Associazione Italiana per la Sicurezza Informatica) nella sua ultima Newsletter.

La ricerca, effettuata in tre fasi, evidenzia inoltre le percezioni dei telelavoratori nei confronti dell'IT manager, e viceversa come l'IT manager pensa di essere considerato dal telelavoratore.

Al fine di comprendere al meglio come le percezioni e il comportamento dei telelavoratori vadano ad intensificare i rischi di sicurezza per l'intera comunità in rete, le aziende IT e le organizzazioni per cui lavorano, la ricerca è stata condotta, in una prima fase, su un campione complessivo di 1.000 telelavoratori e nella seconda e terza fase, su un ulteriore campione di 1.000 IT decision maker nei seguenti 10 Paesi: Stati Uniti, Inghilterra, Francia, Germania, Italia, Giappone, Cina, India, Australia, e Brasile.

I risultati di tale studio mettono in luce le problematiche che i dipartimenti IT si trovano ad affrontare a seguito dei comportamenti pericolosi o a rischio dei dipendenti che lavorano al di fuori dell'ufficio (telelavoro) - una pratica lavorativa che può accrescere la produttività ma che allo stesso tempo può compromettere la sicurezza aziendale.

Prima fase: percezioni e comportamento dei telelavoratori
Lo studio ha rilevato che la maggior parte dei lavoratori mobili è convinta di operare in modo sicuro, nonostante continui ad attuare comportamenti on-line potenzialmente pericolosi.

Alcune evidenze:

· **Shopping online**: Circa il 40% dei telelavoratori intervistati (il 47% in Italia) ha affermato di utilizzare il proprio computer aziendale per fare shopping su Internet. La metà ha affermato di fare personalmente gli acquisti on-line perché "alla loro società non dà fastidio che lo facciano" (41% in Italia).

· **Condivisione dei computer con persone esterne all'azienda**: Il 21% degli intervistati (il 31% in Italia) ha affermato di permettere ad altre persone di utilizzare il proprio computer aziendale. Un intervistato su quattro (il 50% in Italia) afferma di "non vedere niente di sbagliato in questo comportamento" e di essere convinto che l'utilizzo condiviso dei computer "non aumenta i rischi alla sicurezza" (il 13% in Italia).

· **Comportamento wireless pericoloso**: Un intervistato su dieci (il 18% in Italia) ha dichiarato di aver utilizzato la connessione Internet di un vicino, mentre lavorava in remoto. La maggioranza ha affermato di agire in tal modo perché "era una situazione di emergenza." Il 18% degli intervistati (il 21% in Italia) ha affermato "i miei vicini non lo sanno, quindi va bene così."

· **Dispositivi personali**: Circa la metà degli intervistati ha dichiarato di utilizzare i propri dispositivi elettronici personali per accedere alle risorse aziendali. Tuttavia solo la metà degli intervistati (il 29% in Italia) ha detto di avere un software antivirus o di sicurezza installato sul proprio computer.

· **Scaricamento delle e-mail**: Il 38% degli intervistati (il 34% in Italia) ha affermato di aprire e-mail di provenienza sconosciuta ma non gli allegati.

Nonostante i telelavoratori comprendano l'importanza che la sicurezza ricopre per la propria azienda, il loro comportamento suggerisce ai dipartimenti IT aziendali di aumentare il proprio impegno e gli investimenti nella formazione e nella collaborazione con gli utenti. Incoraggiando attivamente una comunicazione bi-direzionale con gli utenti, l'IT manager può compiere un importante passo avanti verso una maggiore comprensione delle strategie di sicurezza aziendali da parte degli utenti.

Seconda fase: Il ruolo dell'IT manager
Sulla base dei dati emersi dal precedente studio, la seconda fase della ricerca ha analizzato due importanti aspetti: le percezioni dei telelavoratori nei confronti dell'IT manager, e -viceversa? come l'IT manager pensa di essere considerato dal telelavoratore.

In sei Paesi su dieci tra quelli sopra citati, i telelavoratori riconoscono ai loro superiori, invece che al dipartimento IT, l'autorità di controllare i loro comportamenti informatici. In generale, il 13% dei telelavoratori dichiara che nessuno all'interno all'azienda ha l'incarico di controllare i dispositivi informatici.

L'Italia è fra le eccezioni: il 49% si affida all'IT manager, il 16% al proprio superiore mentre il 35% dichiara che non è compito di nessuno.

Tali risultati, non hanno invece stupito i professionisti IT intervistati, che dichiarano di essere consapevoli della percezione che i telelavoratori hanno del loro ruolo. Secondo il 53% dei professionisti IT intervistati (il 42% in Italia), gli utenti non riconoscono ai dipartimenti IT la responsabilità di controllare il modo con cui vengono utilizzati gli strumenti informatici dell'azienda.

Terza fase: Gli investimenti nella sicurezza
La terza fase della ricerca, ha invece analizzato l'andamento delle chiamate agli help desk IT e la propensione ad effettuare investimenti nella sicurezza.

Globalmente, il 38% dei decision-maker intervistati (il 42% a livello italiano) ha registrato una crescita delle chiamate all'help-desk per incidenti relativi alla sicurezza che coinvolgono gli utenti e i loro dispositivi informatici utilizzati per lavoro.

Tra le principali cause di tale aumento compaiono: attacchi di virus e/o worm (48% globalmente, 35% in Italia), spyware e/o adware (47% globalmente, 40% in Italia), spam e/o phishing (52% globalmente, 49% in Italia), furto di identità (26% globalmente, 12% in Italia), hacking (28% globalmente, 14% in Italia).

A fronte di tutto ciò, il 67% degli intervistati (il 66% a livello italiano) ha dichiarato di prevedere maggiori investimenti in sicurezza nel corso del prossimo anno, e di questi il 41% (il 34% in Italia) prevede un aumento della spesa superiore al 10%. "Questi dati sono una chiamata alle armi per i dipartimenti IT e Sicurezza," ha affermato Jeff Platon, vice president of security solutions marketing di Cisco. "La ricerca mostra chiaramente che la consapevolezza dimostrata dagli utenti non risulta sempre in un comportamento sicuro, e dal momento che molti utenti rigettano l'autorità dell'IT, non danno credito al proprio team IT né si rivolgono ad esso.

Analizzando questi dati, non sorprende quindi che i dipartimenti IT stiano registrando un numero più elevato di chiamate all'helpdesk e che ci sia una maggiore propensione agli investimenti in sicurezza. Comprendere le motivazioni che sottostanno a tali trend, significa che i responsabili IT devono adottare con urgenza un approccio più progressivo per proteggere i dati aziendali e gli impiegati." "La tecnologia è un importante elemento nella sicurezza, ma non è tutto", ha aggiunto John N. Stewart, chief security officer di Cisco. "La sicurezza è in primo luogo un esercizio umano. Vi è un aspetto interpersonale che coinvolge la comunicazione e un impegno costante nella formazione, educazione e riconoscimento. Creare delle solide relazioni

all'interno dell'azienda permette ai responsabili IT di essere percepiti dall'utenza come una presenza strategica e consulenziale in grado di favorire una cultura aziendale consapevole in fatto di sicurezza. Quando ciò avviene, i CIO e i CSO sono in grado di massimizzare il ritorno dagli investimenti effettuati in soluzioni di sicurezza e di prevenire i pericoli che insidiano la produttività".

"Mai come oggi, la Sicurezza è di così fondamentale importanza per le organizzazioni: le reti rappresentano per qualsiasi impresa lo strumento più importante per ottenere vantaggi competitivi, raggiungere nuovi mercati, creare nuove fonti di reddito e migliorare i livelli di produttività. Tale trasformazione è possibile solo se le infrastrutture e i sistemi informatici sono in grado di garantire adeguati livelli di Sicurezza. Protezione e integrità della rete sono infatti componenti essenziali di ogni strategia di e-business", ha affermato Roberto Mircoli, Security Business Development Manager di Cisco e membro del Comitato Direttivo del CLUSIT. "Sicurezza, infatti, è molto più che prodotti o tecnologie, ed è questo il principio ispirativo dell'impegno dimostrato e mantenuto elevato negli anni da Cisco per la diffusione della cultura della Sicurezza in Italia."

---

www.puntosicuro.it