

## CeBIT 2009: ad Hannover nel mirino della cyber mafia

---

*G Data mette in guardia i visitatori contro attacchi spia e furti di dati*

Il furto e il commercio di informazioni aziendali confidenziali è un lucroso affare per i cyber criminali. Le grandi fiere, come il CeBIT di Hannover, offrono agli hacker un vasto campo di caccia e sono un'ottima opportunità di business per le cyber gang che, secondo quanto valutato da G DATA, prenderanno di mira soprattutto gli utenti di netbook e notebook. La truffa dei criminali: i ladri di dati creano i propri access point e si propongono come provider per hotspot gratuiti agli aeroporti, nelle stazioni e all'interno delle fiere. In questo modo i criminali sono in grado di intercettare l'intero traffico di dati all'interno di una rete. G DATA fa dunque presente i rischi che ci sono nell'utilizzare WLAN non sicure e per ridurre al minimo le conseguenze del furto di dati consiglia quantomeno di fare un back up prima di partire per il CeBIT. Inoltre gli utenti dovrebbero cifrare i propri dati sensibili sull'Hard Disk in maniera tale che soprattutto i dati riservati delle aziende siano protetti contro i tentativi di accesso dei criminali.

'Per i criminali online il traffico di dati è un business milionario. Il prezzo dipende dalla qualità dei dati. Ad esempio un pacchetto di dati indifferenziati del peso di parecchie centinaia di Mbyte può essere venduto anche per meno di 50 dollari.

Naturalmente, per quanto riguarda dati aziendali il valore è significativamente più elevato. Se i criminali cercano di impadronirsi di dati sensibili come piani di costruzioni, risultati di ricerche scientifiche, liste di clienti o business plan, in taluni casi è possibile ottenere anche un profitto di un paio di milioni.', ha spiegato Ralf Benz Müller, Manager di G Data Security Labs.

### 3 suggerimenti per i visitatori del CeBIT

#### 1. Fare molta attenzione quando si usano WLAN pubbliche

Per i criminali è facile proporsi come hotspot WLAN e leggere tutti i dati delle ignare vittime. Se i dati devono per forza di cose essere trasmessi, lo si dovrebbe fare solo in un formato cifrato. Dove possibile, tutto il traffico di dati dovrebbe essere trasportato tramite un tunnel VPN o una connessione UMTS. In questo caso potrebbero essere intercettati solo con uno sforzo decisamente fuori misura.

#### 2. Criptare i dati

I possessori di notebook dovrebbero utilizzare performanti software per la cifratura dei dati o attivare la funzione BitLocker di Windows Vista al fine di rendere i dati del proprio Pc inutilizzabili per i ladri. Oltre a questo è consigliabile utilizzare password più lunghe e complesse. Questo vale anche per i dati su chiave USB e Hard Disk.

La perdita fisica di una periferica può essere grave, ma paragonata con le conseguenze derivanti dalla perdita dei dati è insignificante.

Tutti i dati inoltre che non servono durante il viaggio sarebbe meglio cancellarli dal notebook in

modo da essere ancora più sicuri.

### 3. Proteggere fisicamente I dati

Un lucchetto fisico dovrebbe essere incluso in ogni borsa porta notebook. Questo perlomeno fermerà i ladri occasionali che vorrebbero rubare il Pc dalle nostre mani. Inoltre i Pc portatili non dovrebbero essere lasciati incustoditi anche solo per poco tempo. Dati particolarmente importanti non dovrebbero poi essere salvati sul Pc stesso quanto invece su una chiave USB o un Hard Disk portatile di modo che gli utenti possano portarli sempre con sé ed usarli effettivamente solo quando serve.

**Publicato il:** 02 marzo 2009

**Fonte:** [Sito Ufficiale G DATA](#)

**Autore:** [marco giannatiempo](#)

**Link:** <http://www.gdata.it>

**News inserita in:** [Sicurezza e virus](#)

FullPress.it è una testata giornalistica registrata al Tribunale di Potenza n. 258 del 25.02.99 - FullPress Agency S.r.l. P.Iva e Cod.Fisc. 01334450762 - ©1999-2010 FullPress Agency