



O1net network ▶ O1net Applicando CIO Club IISoftware.it  
 TechTarget Italia ▶ SearchCIO.it SearchSecurity.it SearchNetworking.it



PC Open Digifocus



ricerca: \_\_\_\_\_ in Lineaedp **CERCA** powered by

login:   registrati newsletter blog

O1net Lineaedp LineaedpPMI Computer Dealer & Var Reseller Business Nets

Sistemi | Software | Gestione | Mercati | CIO | Nets | Innovation People | Business Guide: CIO | PMI | Security |



Focus - Sicurezza - da Lineaedp 14/15-09

## Consigli Pratici per tutelare le informazioni e l'azienda

*Intervista a Paolo Graziano, amministratore delegato di Formedia, società con una significativa esperienza consulenziale nell'ict*

[Laura Zanotti](#)

Un aspetto critico che impatta sulla sicurezza aziendale è la sempre maggiore pervasività della consumerization, ovvero l'utilizzo di tecnologie o approcci consumer all'interno dell'azienda, che includono attività di social networking così come l'utilizzo di palmari e apparati che non sono forniti dall'azienda e che, malgrado non siano allineati a determinate policy aziendali, vengono utilizzati anche per fare business, dipanando tutta una serie di flussi informativi in entrata e in uscita correlati all'azienda. Si tratta di un'evoluzione tecnologica che impone un ripensamento della governance, finalizzata a dotare di una sicurezza adeguata tutti i rapporti che avvengono tra partner, dipendenti e fornitori. Le minacce sono sempre meno prevedibili, le loro caratteristiche sono mutanti per cui bisogna giocare di anticipo. Oltre alle tecnologie di autenticazione, che rimangono importanti, va migliorata la sicurezza dei dati che sempre più vengono utilizzati da interlocutori diversi. Nata a Milano nel 1997, Formedia è una società che vanta una lunga esperienza in merito alla variegata casistica dei problemi informatici aziendali, offrendo un'attività di servizio che comprende consulenza e assistenza, sia hardware che software, progettazione di reti informatiche, realizzazione di siti Web, e-marketing, supporto alle normative vigenti in termini di sicurezza e di compliance. Rispetto ai dati e alle analisi di mercato, Paolo Graziano, in qualità di amministratore delegato Formedia, ha una visione decisamente più ravvicinata delle specificità che connotano il modus operandi aziendale italiano, come ci spiega in questa intervista.



### Qual è l'atteggiamento delle imprese verso la security?

«Indipendentemente dalla tipologia del business e dalle dimensioni, innanzitutto c'è la consapevolezza che da Internet arrivano le infezioni per cui è necessario l'antivirus. Quando si spiega alla direzione aziendale che l'antivirus non è un metodo di sicurezza ma un tool che qualunque computer deve avere, scatta la prima domanda: "esiste una versione gratuita"? Di fronte a un elenco delle differenze sostanziali tra una versione gratuita che, in ogni caso, non è possibile usare in un ambiente di lavoro, e una a pagamento allora le aziende capiscono che non hanno capito nulla, fino a quando non capita un grosso problema: per esempio il virus che ha bloccato le connessioni di rete, di conseguenza non è possibile accedere ai dati che, non arrivando più sul server, impediscono la stampa delle fatture. A questo punto viene percepita chiaramente la necessità della sicurezza. Molte aziende sono proattive, ma mi è anche capitato di perdere ore a discutere se fosse il caso di investire un migliaio di euro per proteggere una cinquantina di computer perché ci volevano le licenze. Quando sono riuscito a spiegare che una ventina di euro a macchina e all'anno per avere un ambiente protetto significa risparmiare due giornate/uomo di lavoro necessarie per riattivare il fermo salvando i dati, l'investimento è stato sbloccato. Lo

### TUTTI I NUMERI di Lineaedp

CIO Club  
 ProntoImprese

Webcast  
 Security 2.0 e DLP  
 Protezione dei dati aziendali

Sfatiamo i falsi miti sui blade server

Idc, la roadmap verso l'azienda virtualizzata

Le Top 200 dell'IT in Italia 2008

Giro di poltrone

TIPS & TUTORIAL by TECHTARGET  
 Professionisti di sicurezza  
 Responsabili IT  
 Tecnici di rete

I corsi di formazione

Eventi e Appuntamenti IT e TLC

Link utili  
 Passepartout  
 Software  
 Gestionale  
 Compara Prezzi  
 Portale immobiliare  
 News e servizi per gli operatori dell'edilizia  
 Il sito per architetti e designers  
 News e servizi per l'agroindustria  
 Business News sul mercato del Retail  
 Dossier e aggiornamenti su marketing e distribuzione

spamming è il secondo problema che affligge le aziende e che, detto per inciso, al di là dei sistemi di protezioni, implicherebbe un percorso di educazione dei dipendenti, i quali dovrebbero imparare a non lasciare i loro riferimenti quando navigano liberamente in rete dall'ufficio».

*Il problema è che quando si parla di piani di sicurezza il rapporto tra costi e benefici non è evidente.*

«La sicurezza non è qualcosa di tangibile ma spesso, anche quando esiste un progetto, questo è approssimato: i backup non vengono fatti regolarmente, spesso si scopre che comprendono solo alcune procedure e che in pochi casi viene fatto il restore. A campione, saltuariamente, bisognerebbe cancellare una macchina e ripristinarla tramite sistemi di backup ma posso affermare che sono in pochi a effettuare questa simulazione di rischio. Un caso recente capitato a un mio cliente è quello di un dipendente che si è licenziato e, prima di andarsene, ha formattato il suo computer: per cui tutto quello che c'era su quella macchina è andato perso. Avendo toccato con mano il rischio, l'azienda ha reagito programmando un piano serio di backup, con controlli degli stessi, password di accesso, limitazione all'utente sulla password di accesso, naturalmente nel rispetto dei limiti della legge che tutela i diritti dei lavoratori, e completa messa in sicurezza delle informazioni. Controllare gli accessi non è una banalità: può capitare che le informazioni possano essere cancellate per incuria o per dispetto. Il ragionamento che si deve fare è lo stesso di quando si stipula una polizza assicurativa per l'automobile: ci si tutela da una serie di rischi che non è detto che possano accadere, ma se accadono è necessario essere in sicurezza».

*Il virus è evidente ma il malware è subdolo, operando in modo latente. Quanto sanno le aziende delle modalità attraverso cui opera la pirateria?*

«La Rete è mondiale e gli hacker, che stanno in tutto il mondo, non hanno nazionalità. Nel momento in cui viene lanciato uno sniffer, questo va a controllare tutti gli indirizzi Ip richiesti, senza controllare patria o paese. Se l'obiettivo, ad esempio, è quello di carpire più informazioni possibili sulle carte di credito l'hacker, cercando di farsi notare il meno possibile, opera sulla macchina che è riuscito a penetrare installando una serie di programmi, che non sono virus ma che iniziano a carpire informazioni. Può essere il caso di un algoritmo capace di leggere le sequenze numeriche alla ricerca di una stringa caratteristica di una carta di credito. Esistono algoritmi programmati per cercare tutti gli indirizzi di posta elettronica presenti su una macchina, usandola come ponte per aggredirne delle altre, magari agganciandosi a una mail che viene inviata e che, nel momento in cui viene scaricata, fa comparire sulla macchina un pezzettino di codice che automaticamente si collega al Web e scarica il resto del programma che gli serve per attivarsi. È difficile far capire alle aziende che, paradossalmente, l'unico computer sicuro è un computer spento, chiuso in una stanza di cui si è buttata via la chiave. Dal momento che in azienda i computer sono accesi, è necessario implementare tutta una serie di sistemi di sicurezza attivi: un firewall, ovvero un sistema che intercetti tutte le chiamate in ingresso per fare passare solo determinate informazioni e, dall'altra un proxy, cioè un sistema che dall'interno dell'azienda controlli e possa eventualmente vincolare gli accessi che dall'interno dell'azienda vengono fatti verso l'esterno. Ora firewall e proxy esistono come software gratuiti in Linux, con dei costi di installazione, di gestione e di utilizzo; sempre più aziende stanno orientandosi verso questo tipo di approccio. Un'azienda attaccata da uno spamming selvaggio, con una media tra le 4.000 e le 6.500 mail al giorno aggredite da spam contenenti virus ha risolto il problema implementando un antispam a costo zero su Linux in ambiente Vmware. Utilizzando la macchina virtuale, quattro pulsanti di configurazione e lo spamming è stato neutralizzato. L'installazione richiede certamente una persona capace ma i tempi sono assolutamente rapidi e i costi minimi. E questi sono risultati immediatamente tangibili per il Cda aziendale. La tendenza è quella di preferire di pagare poco o niente un prodotto e di affidarsi a un partner tecnologico che, a pagamento, offre tutto il supporto correlato».

*Dal momento che il terrore corre sul Web i provider potrebbero proporsi come partner della sicurezza?*

«I provider possono giocare un ruolo importante nella costruzione della sicurezza, in quanto detentori di un certo livello di skill e di tecnologie che possono erogare sicurezza alle aziende senza necessità di formazione aggiunta. La sicurezza a pacchetto sta, infatti, diventando una formula strategica; la dirigenza è più predisposta a un "chiavi in mano" con una quota fissa mensile. Oggi ritengo che il bundle connessione/sicurezza sia molto vincente. Anche in questo caso bisogna stare attenti agli standard utilizzati, perché mi è capitato di avere clienti che mi chiedevano aiuto in quanto la user name a loro assegnata era più lunga del campo utente a disposizione...».

*Sul fronte della protezione dei dati e della privacy, le policy sono state calate dall'alto, a livello governativo. Butler Group sul tema della sicurezza ha evidenziato una lista di priorità che oltre a comprendere l'obbligo di rispettare leggi e normative relative all'Iso-17799/Bs 7799-2/Cobit, mette al secondo posto il Codice di protezione dei dati personali e al terzo il Documento programmatico sulla sicurezza (Dps).*

«La normativa sulla privacy, tradotta in legge e ridotta a un concetto di documento sulla privacy, chiamato Dps, è una procedura che tutte le aziende di ogni ordine e grado in Italia hanno l'obbligo di porre in atto attraverso la redazione di un documento da aggiornare annualmente. Da quest'anno sono state realizzate delle soglie diverse, per cui le realtà più piccole possono autocertificarsi mentre prima, sia la multinazionale che la ditta individuale dovevano redigere il medesimo documento. La differenza scatta nel momento in cui il dato personale diventa dato sensibile: finché si rimane nel campo di un'anagrafica con nome, cognome e indirizzo, telefono, partita Iva e codice fiscale che servono per operare a livello commerciale in Italia si ha l'obbligo di

informare il cliente del fatto che si conoscono e trascritto sul nostro computer queste informazioni e che quest'ultime verranno gestite con accuratezza: per cui esiste un sistema di tracciamento, si fanno backup con regolarità, ci sono persone autorizzate e controllate che accedono secondo procedure di sicurezza a queste informazioni, l'ambiente è protetto da sistemi antincendio e, nel caso, antifurto, i sistemi di archiviazione seguono procedure specifiche e via dicendo. Quando il dato diventa sensibile, cioè rimanda a una conoscenza implicita di razza, religione, salute e così via, allora scatta la severità della legge, per cui deve essere fatta un'informativa al garante, bisogna dichiarare esattamente cosa si fa e realizzare dei sistemi che rendano il più anonimo possibile questo tipo di informazioni. È capitato che alcune aziende abbiano esplicitamente richiesto di fare una codifica anonima per i faldoni esposti al pubblico, attraverso un sistema di codifica particolare ma esiste anche chi non ha fatto nulla. Sul Dps le aziende dovrebbero farsi un esame di coscienza e inquadrare bene il significato di protezione e di business continuity. Avere un pieno monitoraggio di chi mette le mani sui computer e a quali tipologie di dati queste persone hanno accesso rientra in una logica che va ben oltre il Dps, la privacy e le leggi in materia. L'autocertificazione deve essere fatta con responsabilità, in quanto è necessario stilare comunque un documento in cui si specifica una procedura aziendale che definisce le modalità di intervento in caso di perdita di dati, cancellazione accidentale, interruzione della continuità operativa. Solo così l'autocertificazione è reale, altrimenti è un falso. Certo è che se questo documento viene fotocopiato di anno in anno uguale a se stesso, il suo valore decade. Alcune aziende l'hanno preso sul serio, chiedendo addirittura di specificare sul Dps la presenza di estintori a sufficienza in base ai metri quadri dell'ufficio. Va specificato che in questo caso le leggi si sovrappongono, perché il legislatore dispone e impone l'uso di sistemi antincendio per un ufficio di una data metratura e il Dps, sotto questo profilo, costituisce un richiamo a una normativa preesistente».


[Stampa](#)

[Invia un commento](#)

[Invia questo articolo](#)

I focus di Lineaedp: Tlc - Sicurezza - Business intelligence - Rfid - Enterprise 2.0 - Erp



Data center  
e server blade,  
sfide e opportunità



Chi siamo | Il nostro codice di comportamento | I nostri prodotti | I nostri riferimenti | Pubblicità su O1net Network

Datacenter  
e connettività



#### [Virtualization Management](#)

Open source management of virtualization technology made easy  
[www.groundworkopensource.com](http://www.groundworkopensource.com)



#### [Top 50 ERP & MRP Systems](#)

Get Free ERP Evaluation Reports for Software Selections & Comparisons!  
[ERP.SoftwareResearchTools.com](http://ERP.SoftwareResearchTools.com)

#### [SDA Bocconi](#)

Programmi per gestire Supply Chain e flussi di Logistica Distributiva  
[www.sdabocconi.it/SCM](http://www.sdabocconi.it/SCM)

Annunci Google