

attivi, più di 100 milioni di articoli nuovi in vendita e 5 milioni di acquirenti. Il 67% dei venditori professionali commercializza i propri prodotti all'estero.

come il nostro Mezzogiorno sia particolarmente dinamico; la Campania è in cima alle classifiche di eBay e ha anche la concentrazione di venditori professionali più gran-

in ogni paese in cui opera - risponde Voce - nel rispetto delle norme fiscali previste a livello locale, europeo e internazionale, incluse le normative Ocse sull'e-commerce».

lizzandosi in Information technology. Nel 2007 ha iniziato a lavorare in PayPal e in eBay. Per oltre cinque anni ha guidato la gestione delle vendite e lo sviluppo di business

to Italia e Spagna come primi paesi in Europa. «In eBay c'è un team di manager che non solo funge da esempio e da cui c'è tanto da imparare, ma che ti aiuta nella crescita,

57 milioni di di euro. «Con tante storie di aziende che rischiavano di chiudere e si sono rilanciate».

© RIPRODUZIONE RISERVATA

# Sanità digitale a rischio cyberattacchi troppo It "ombra" e investimenti al palo

**I RISULTATI DELLO STUDIO NETICS CHE VERRÀ PRESENTATO MERCOLEDÌ AL FORUM S@LUTE: PRIVACY DEI PAZIENTI IN PERICOLO SE I MEDICI USANO PROGRAMMI E PC PERSONALI**

Stefano Carli

Roma

La sanità digitale in Italia non è sicura: i dati dei pazienti sono a rischio privacy, la sicurezza delle cartelle cliniche, l'anagrafe sanitaria di ciascuno di noi, è a rischio di attacchi informatici. E in generale il settore sanitario italiano è quello che più di tutti fa ricorso in Europa al cosiddetto Shadow It, il software ombra: non è altro che l'uso di software non ufficiale, non standardizzato e spesso non sicuro per conservare, organizzare, gestire e trasmettere documentazione digitale sanitaria, risultati di analisi, immagini diagnostiche. E' l'allarme che verrà lanciato ufficialmente al governo e al settore pubblico mercoledì e giovedì prossimi a Roma in occasione di S@lute, il Forum dell'Innovazione per la salute i cui lavori saranno aperti dal ministro Beatrice Lorenzin. In quell'occasione verranno presentati i risultati dell'indagine condotta da Netics tra Asl e ospedali e che tratteggia un quadro ancora dominato da sostanziali ritardi: il 19,7% di Asl e Ospedali (ne so-



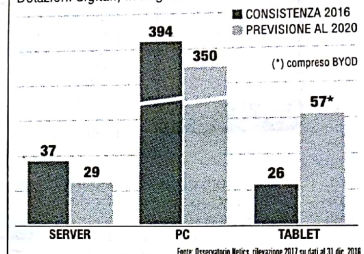
no stati intervistati una cinquantina) dichiarerà di non essere in grado di ripristinare entro 4 ore i propri sistemi It in caso di cyber attack; il 41,6% di responsabili di Asl e ospedali denuncia una allarmante espansione dell'uso di shadow It da parte di medici ospedalieri, accrescendo così le ossibilità per i pirati informatici di poter penetrare nei server delle strutture sanitarie pubbliche; quasi uno su due tra i medici di medicina generale non considera rilevante la minaccia informatica e quasi

altrettanti non fanno backup quotidiani dei dati dei loro server di laboratorio.

Il problema, secondo Paolo Colli Franzone, responsabile scientifico dell'Osservatorio Netics, che presenterà la ricerca al Forum S@lute, è fondamentalmente nella scarsità di budget. «Sono aumentate le postazioni pc connesse al web e non solo alle intranet negli ospedali e nelle Asl, aumentano i server e con tutto questo aumenta l'esposizione al rischio. Non dimento-

## L'IT DI ASL E OSPEDALI

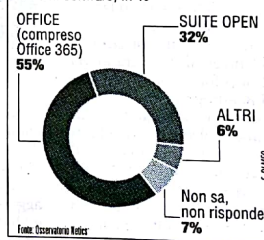
Dotazioni digitali, in migliaia



Il ministro della Salute **Beatrice Lorenzin** Aprirà il Forum S@lute mercoledì prossimo a Roma

## LE DOTAZIONI INDIVIDUALI

Sistemi software, in %



chiamo che il comparto sanitario è al secondo posto, subito dopo la finanza, come obiettivo di azione di ackeraggio sia come furto di dati che come azioni di ricatto, infettando le reti informatiche di Asl e soprattutto ospedali con ransomware per ottenere un riscatto».

Troppe volte i medici sono quindi costretti a surrogare la mancanza di software ufficiali con pc e programmi pagati di tasca propria, o quando possibile accedendo a software gratuiti open source. «È un rischio potenziale notevole - continua Colli Franzone - perché non si sa come lavorino questi software, se i produttori che li immettono gratis sul mercato abbiano accordi per la rivendita dei dati raccolti, o se abbiano anche solo dei banchi che costituiscono porte spalancate agli hacker».

Infine c'è un rischio privacy. Software non sicuri e dal crittaggio non certificato, permettono alle comunicazioni tra medici o tra medici e pazienti di essere preda dei data miner, algoritmi che dragano il web alla ricerca di informazioni per parole chiave, per venire a scoprire cosa ogni utente cerca o acquista, in modo da alimentare i profili personalizzati da vendere alla pubblicità.

© RIPRODUZIONE RISERVATA