

## Comunicato stampa

L'Osservatorio nazionale per la Sicurezza Informatica: molti dati sulla salute degli italiani sono a rischio.

Da una indagine compiuta su alcune ASL, il 60% dei sistemi informatici sono facilmente penetrabili.

Da un'indagine condotta dall'Osservatorio nazionale sulla sicurezza informatica il 60% delle aziende ospedaliere italiane potrebbero avere gravi problemi di sicurezza informatica. Ormai è sempre più diffuso l'utilizzo della rete internet per migliorare il servizio ai cittadini, ad esempio prevedendo la possibilità di ricevere i referti o le cartelle cliniche attraverso il PC. Un servizio importante, che però espone le aziende ospedaliere a possibili problematiche di security.

Da un'indagine condotta su un campione di 50 Asl, risulta che:

- il 100% delle aziende ospedaliere usa internet
- il 82% delle Asl dichiara di essere a norma con la legge sulla privacy, sia dal punto di vista formale e tecnico
- il 60% delle Asl ritiene comunque di non avere strumenti adeguati per la protezione dei dati sensibili
- l'85% delle aziende ospedaliere ha importanti problemi di budget da destinarsi all'IT

“ E' importante che le aziende ASL ed in genere chi opera nella sanità implementi i servizi attraverso internet: si tratta di uno strumento straordinario che permette di abbattere liste di attesa, file, congestione di uffici, e che permette anche di semplificare la vita agli utenti. Il problema però è cercare di usare la tecnologia internet al meglio, cercando di ridurre al minimo la possibilità di furto di dati. – ha dichiarato Mirko Gatto, della Yarix – Non bisogna vedere la sicurezza informatica come un optional, ma come uno strumento essenziale per impedire l'azione dei malintenzionati, soprattutto in un settore delicato come quello sanitario, nel quale si trattano dati molto sensibili. Per questo il consiglio è di rivolgersi ad aziende altamente specializzate in sicurezza informatica, per un monitoraggio delle problematiche possibili e per l'identificazione delle soluzioni percorribili.”.