

31 luglio 2017	
Online	

Home > Prodotti > Sicurezza > Wi-Fi in albergo: come difendersi da DarkHotel

Prodotti Sicurezza

Wi-Fi in albergo: come difendersi da DarkHotel

31 luglio 2017

[Condividi su Facebook](#)
[Tweet su Twitter](#)
[G+](#)
[in](#)
[p](#)




DarkHotel è un'organizzazione hacker che da anni prende il controllo dei dispositivi elettronici, per appropriarsi dei segreti aziendali degli di un hotel, penetrando nel Wi-Fi.

Si tratta di un **malware** camuffato da aggiornamento software oppure, come avvenuto recentemente, contenuto in un'email di **phishing**.

Se da una parte, un'attività di formazione da parte dei responsabili della sicurezza dovrebbe essere effettuata a livello di top management, per evitare rischi al di fuori dell'azienda, dall'altra, gli stessi hotel dovrebbero fare uno sforzo maggiore per affrontare la situazione e migliorare la sicurezza della rete nelle strutture di competenza.

*"Visti i continui attacchi informatici è di assoluta importanza per il settore Ho.Re.Ca mantenere aggiornata la protezione dei dispositivi di rete, per tutelare la propria clientela – dice in una nota Valerio Rosano, Country Manager di **ZyXel Communications** Italy –. Con l'entrata in vigore del GDPR le aziende dovranno identificare il prima possibile le modifiche da apportare ai propri processi di sicurezza".*

 [Iscriviti alla newsletter](#)



Twitter

01net.it @01netIT 1 Aug
 .@4wardIT partner dell'anno per il cloud di @microsoftitalia
 01net.it/4ward-partner-...
 Espandi

 [Segui @01netIT](#) 2.779 follower

Speciale



5G: le mosse di aziende e operatori

20 luglio 2017

A che punto è il 5G in Italia? Ne abbiamo parlato con chi lo dovrà implementare. C'è tutto:

Aggiornare i dispositivi all'ultima versione

All'atto pratico, come ci si difende dal malware negli hotel? Per Zyxel è di assoluta importanza mantenere costantemente aggiornata la protezione dei dispositivi di rete.

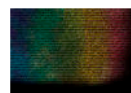
Per esempio, se la struttura alberghiera è in possesso di uno **ZyWall Usg** e utilizza servizi antivirus e Intrusion Detection e Prevention (IDP) abilitato, bisogna verificare che il firmware del device sia aggiornato all'ultima versione disponibile. Poi va abilitato l'anti malware: il **gateway** intercetta i malware al loro primo punto di ingresso, prevenendone così la diffusione all'interno della rete. Ma il firmware deve essere aggiornato all'ultima versione disponibile, necessaria, per esempio, a gestire la problematica del **ransomware** Inexsmar.

> Trend



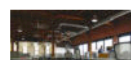
Credito d'imposta su investimenti pubblicitari su quotidiani e periodici

Mercato 27 luglio 2017



Ibm Research: tutte le innovazioni

01net Focus 27 luglio 2017



Cisco e Intesa Sanpaolo chiamano le startup per