

Perché gli Hotel sono il bersaglio preferito dai cybercriminali?

Piccola guida sull'importanza
di proteggere i dati dei tuoi ospiti



Business Provider
COREUP



Gli hacker prendono di mira **hotel e portali di prenotazione** perché sono una fonte importante di dati sensibili e di transazioni con le **carte di credito**. Solitamente il mondo hotellerie ha livelli di sicurezza informatica inferiori rispetto a una banca: questo rende il settore hospitality **più facilmente attaccabile**.

Un hotel medio gestisce la maggior parte delle sue attività online: prenotazioni, transazioni economiche, accesso alle camere, video sorveglianza, irrigazione, e molto altro ancora. Negli hotel con servizi automatizzati, un fermo del sistema significa un blocco dell'intera struttura, ospiti insoddisfatti e un ritorno di immagine negativo.

In caso di incidente IT, la tua struttura ricettiva sarebbe in grado di dimostrare di aver applicato ogni possibile protezione in modo costante?

I tuoi collaboratori sarebbero nelle condizioni di riprendere il lavoro senza interruzioni (Disaster Recovery Plan e Business Continuity)?



Le minacce informatiche al settore Hospitality:

Questi sono alcuni dei **cyber attacchi** più diffusi che coinvolgono l'hospitality: Phishing (invio di e-mail apparentemente sicure), Ransomware (attacco a scopo di riscatto), DDoS (sistema in tilt e blocco delle funzioni automatizzate), Point of Sale (attacco dai terminali di pagamento) con conseguente:

- **Furto dei dati sensibili:** carte di pagamento, informazioni personali, informazioni bancarie, furto d'identità.
- **Intromissione nei sistemi di gestione** della struttura: è capitato, ad esempio, che un gruppo di hacker prendesse il controllo del sistema automatico di apertura delle porte delle stanze chiudendo fuori centinaia di ospiti e chiedendo un riscatto per riportare la situazione alla normalità.
- **Intromissione nei sistemi di videosorveglianza:** gli hacker possono mettere a repentaglio la tranquillità degli ospiti dato che molte procedure sulla sicurezza sono automatizzate (e quindi attaccabili).

Questione di sicurezza (ma anche di reputazione)

Una riflessione: Che sia vacanza o viaggio di lavoro, quello che gli ospiti cercano fuori casa sono **comfort e sicurezza**. Se il primo punto è soggettivo, non lo è sicuramente il secondo: la sicurezza va garantita nel rispetto della normativa e della fiducia della clientela.



È bene quindi ricordare che un hotel sotto attacco hacker dovrà gestire sì il problema del furto di dati sensibili, ma anche la questione **reputazionale**: se una struttura viene percepita come “non sicura” i clienti prenoteranno altrove e, con molta probabilità, troveranno posto vista l'offerta così ampia.

Investire nella sicurezza informatica fa bene alla tua attività: oltre che sui servizi offerti, puoi puntare sul tema della **cybersicurezza** come tratto distintivo della tua struttura. Far sapere che proteggi i dati sensibili dei tuoi ospiti con sistemi sempre aggiornati ed efficienti ti aiuterà ad emergere nel mare magnum della concorrenza.

CONSIGLIO: Investi nella sicurezza IT, informa i tuoi clienti e usala come leva di marketing per distinguerti dai concorrenti.

Hotel Cybersecurity: come proteggersi

Core Up Srl suggerisce alle aziende operanti nel settore HOSPITALITY di compiere le seguenti azioni strategiche:



A. Praticare l'igiene informatica

Si tratta di un insieme di buone pratiche interne che riducono il rischio legato a virus e attacchi hacker. Molto spesso la fonte di un virus è proprio la chiavetta usb di un collaboratore, lo sapevi? Anche le e-mail di phishing vengono inconsapevolmente attivate dal personale interno. Ecco perché occuparsi della formazione interna (cyber awareness) sui rischi e sulle norme di igiene informatica è il primo passo da compiere (Core Up propone corsi personalizzati).

B. Scegliere un MSP

Per la **gestione**, il **monitoraggio** e la **salute** dell'ambiente IT del tuo hotel si può incaricare un MSP Managed Service Provider (Provider di servizi gestiti) che **da remoto e 24/7 controlla** lo stato delle reti e dei sistemi. Un MSP compie tutte quelle azioni necessarie a tenere il più possibile in sicurezza l'infrastruttura IT (rinnovo dell'antivirus, installazione di firewall, manutenzione hardware...) e, in caso di attacco o problemi, interviene tempestivamente per riportare la situazione alla normalità.

C. Verificare la sicurezza dell'infrastruttura IT

Per identificare le minacce IT e mitigarne i rischi, è fondamentale partire da una **valutazione della sicurezza** dell'infrastruttura attraverso due tipologie di verifica: il Vulnerability Assessment e il Penetration Test sono metodologie (complementari e consequenziali) che permettono di realizzare un **Security Program** su misura, efficace ed efficiente. (Un MSP si occupa anche di questo!)

D. Studiare una strategia di gestione in caso di incidenti IT

Pensare a un piano di azione concreto ed efficiente aiuta a **mitigare i problemi** in caso di incidenti informatici che mandino in tilt i sistemi IT con conseguente perdita dei dati o furto di informazioni sensibili. (Anche in questo caso scegliere un MSP si rivela una scelta vincente!).

Managed Service Provider (MSP): chi è?

Un MSP aiuta a **proteggere i dati sensibili** e il know-how aziendale con il monitoraggio costante dell'ambiente IT, la manutenzione e la gestione proattiva.

In caso di attacchi o disastri IT l'azienda riparte nel minor tempo possibile, riducendo quindi i **tempi di fermo** e le perdite economico-finanziarie.

Offre servizi altamente specializzati su base contrattuale, spesso con un **canone** mensile/annuale, permettendo al cliente di esternalizzare le complessità tecnologiche e concentrarsi sul proprio core business.

Dati sensibili al sicuro: Imprenditori liberi di concentrarsi sul fatturato

Quando hai un partner IT con funzione di MSP puoi contare su un'infrastruttura IT **efficiente e sicura** mentre ti dedichi al tuo lavoro.

In caso di incidente IT dovuto a un attacco hacker, a un errore umano o a un disastro naturale, un MSP ti aiuta a contenere i danni e le perdite perché ti permette di ripartire nel minor tempo possibile, scongiurando i tanto temuti down-time.

Inoltre, se scegli un MSP che fornisce anche hardware e software, avrai un parco macchine IT sempre aggiornato e performante.

I vantaggi per le aziende che scelgono un MSP:

- Continuità operativa e riduzione dei tempi di fermo
- Assistenza telefonica e da remoto illimitata
- Rete IT più sicura e sempre aggiornata
- Unico referente IT: risparmio di tempo/denaro
- Consulenza IT altamente qualificata
- Zero sorprese di spesa: comodo contratto con canoni periodici fissi
- Rinnovo parco macchine con comoda formula noleggio

E se capitasse alla tua struttura ricettiva?

2017, Romantik Seehotel Jaegerwirt, Austria

L'hotel è dotato di un sistema automatizzato di apertura e chiusura delle porte delle stanze: gli hacker sono entrati in questo sistema, controllandolo. 180 ospiti sono rimasti chiusi fuori dalle loro camere fino al pagamento di un riscatto.



2018, Prince Hotels Inc, Giappone

Uno dei più grandi operatori di hotel e resort della nazione ha subito un attacco hacker che ha portato al furto di dati sensibili di quasi 125.000 clienti che avevano prenotato le camere tramite il sito ufficiale in lingua straniera.

2023, MGM Resorts, USA

È bastata una telefonata di pochi minuti per mandare al tappeto questo colosso da 33 miliardi di dollari: gli hacker hanno contattato l'helpdesk dell'azienda fingendo di essere un dipendente e chiedendo di resettare la password del profilo utente. L'attacco ha minato i sistemi di prenotazione, le chiavi elettroniche delle camere, i bancomat e le slot machine. La causa principale di questo disastro è stata la mancanza di una strategia di difesa dagli attacchi cibernetici, sottovalutando quindi i rischi a cui l'azienda era esposta.

“Noi siamo piccoli, a noi non capita.”

“Abbiamo l'antivirus, siamo tranquilli.”

“Tanto facciamo il backup su hard disk.”

Queste frasi rappresentano un rischio per molti Studi.

Nessuno è troppo piccolo per essere attaccato:

le minacce informatiche ormai si muovono in modo automatizzato, colpendo chiunque abbia una vulnerabilità aperta, indipendentemente da dimensione o fatturato.

Core Up: il tuo MSP, e non solo...

Scegliere un **partner tecnologico MSP** come Core Up, che propone il noleggio e la vendita di hardware e software per l'ufficio e servizi di monitoraggio, assistenza e gestione proattiva dell'infrastruttura IT, **aumenta i livelli di sicurezza** del tuo Studio, riducendo al minimo i tempi di down-time e i disservizi. Così potrai ottimizzare tempi e costi, il tutto gestito con comodi canoni periodici personalizzabili.

Cosa possiamo fare per te:

- **SERVIZIO DI MSP (MANAGED SERVICE PROVIDER)** per il monitoraggio e la gestione proattiva della tua infrastruttura IT
- **NOLEGGIO DI PC, SERVER, STORAGE, STAMPANTI E MULTIFUNZIONI per ufficio/reception** con comodi canoni periodici personalizzabili per un ambiente IT sempre aggiornato e performante
- **TELEFONIA E CONNETTIVITÀ**
- **TECNOLOGIE PER MEETING ROOM** per le sale congressi del tuo hotel



Contattaci per maggiori informazioni: sarà un piacere conoscere la tua realtà e consigliarti i migliori strumenti per far crescere il tuo Studio.

T. 030.4194040

M. info@coreup.it / segreteria@coreup.it

W. www.coreup.it

seguici di LinkedIn:

