ergonomic solutions

PCI Security Standards Council
PARTICIPATING ORGANIZATION™

Il tempo sta per scadere

La protezione fisica dei vostri dispositivi di pagamento non è più una semplice opzione.

I retailer che pensano che la data ultima del 30 giugno 2015 per mettersi in regola non li riguardi devono ricredersi e AGIRE ORA.

La protezione fisica dei terminali di pagamento diventa obbligatoria dal 30 giugno 2015. Le organizzazioni hanno meno di sei mesi per mettersi in regola con PCI DSS V3.0 Requisito 9.9, pena una serie di gravi sanzioni pecuniarie e una pubblicità potenzialmente dannosa.

CHI SIAMO

Ergonomic Solutions è specializzata nella sicurezza dei pagamenti. Quando EMV (Chip & PIN) è stato lanciato in Europa, i nostri supporti di pagamento SpacePole® hanno definito lo standard internazionale. A tutt'oggi abbiamo fornito oltre 2 milioni di soluzioni in tutta Europa.

Mantenersi un passo avanti

La sicurezza è al centro di ogni operazione di pagamento. La crittografia point-to-point (P2PE) assicura la protezione dei dati, ma lo skimming dei dispositivi è ancora un rischio. Si stima che 5.000 terminali per volta possano essere messi all'asta, completi dei dati dei consumatori. L'ultima linea di difesa è sempre il retailer e la sicurezza fisica, finora solo una "buona pratica", diverrà ora obbligatoria.

Siamo fidati partner dei principali fornitori di dispositivi di pagamento quali Verifone, Ingenico, ATOS Worldline, Gemalto, Guglia, REA e Miura. Una gamma completa di soluzioni modulari e personalizzate è stata progettata, sviluppata e prodotta per le loro suite di dispositivi di pagamento statici e mobili.

Questa guida vi dirà tutto quello che dovete sapere per elaborare la vostra tabella di marcia nel periodo antecedente la scadenza del 30 giugno 2015.

LA VOSTRA ORGANIZZAZIONE HA BISOGNO DI AGIRE

Ogni impresa che riceve pagamenti da parte dei clienti attraverso un dispositivo di pagamento fisico ha tempo fino al 30 giugno 2015 per mettersi in regola con PCI DSS Version 3.0 Requisito 9.9. Pubblicata nel novembre 2013, in risposta ad un continuo incremento delle manomissione e violazioni dei dati, stabiliva una serie di requisiti, tra cui:

"Proteggere da manomissioni e sostituzioni i dispositivi che acquisiscono dati delle carte di pagamento attraverso l'interazione fisica diretta con la carta"

(pagina 79 della direttiva)

Questa è considerata una buona prassi fino al 30 giugno 2015, dopo di che diventa obbligatoria, per cui gli esercenti dovranno:

Addestrare il proprio team di gestione e i cassieri in modo da sensibilizzarli alle minacce e affinché imparino ad affrontarle

Implementare nuove procedure di inventariazione regolare dei POI (point-of-interaction) e ispezionarli visivamente per verificare che non siano stati manomessi

Introdurre delle basi di bloccaggio per ogni POI in modo da fissarli al punto vendita

(Prevenzione della strisciata: buona pratica per gli esercenti v.2.0)

NON FARE NULLA NON È UN'ALTERNATIVA PRATICABILE

Qualsiasi violazione della sicurezza dei dati delle carte di pagamento ha conseguenze di vasta portata sulle organizzazioni coinvolte, che possono includere:

- Potenziali multe fino a €300,000 all'anno in caso di inosservanza
- Implicazioni finanziarie delle perizie informatiche a seguito di una violazione dei dati
- Obblighi normativi di segnalazione
- Perdita di reputazione quando le violazioni dei dati sono rese pubbliche
- Perdita di clienti che perdono fiducia nel retailer

Jeremy King, Direttore Internazionale del PCI Security Standards Council ritiene che il costo medio ,per record, di dati di titolari di carta perso nel Regno Unito sia di £ 79 (€ 99).

FATTO

VISA eleva multe fino a **€395,000** per incidente se non si risulta in regola al momento dell'incidente

Una violazione della sicurezza potrebbe costare fino a

€40,000

solo per una perizia informatica PCI

La vostra organizzazione deve pagare la sostituzione di

OGNI

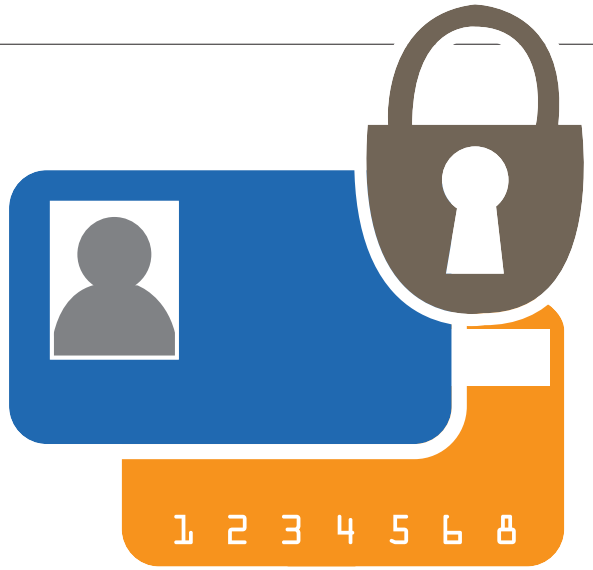
carta compromessa

Tutti i terminali compromessi **DEVONO essere sostituiti**

LE MINACCE CONTINUANO A CRESCERE E AD EVOLVERSI

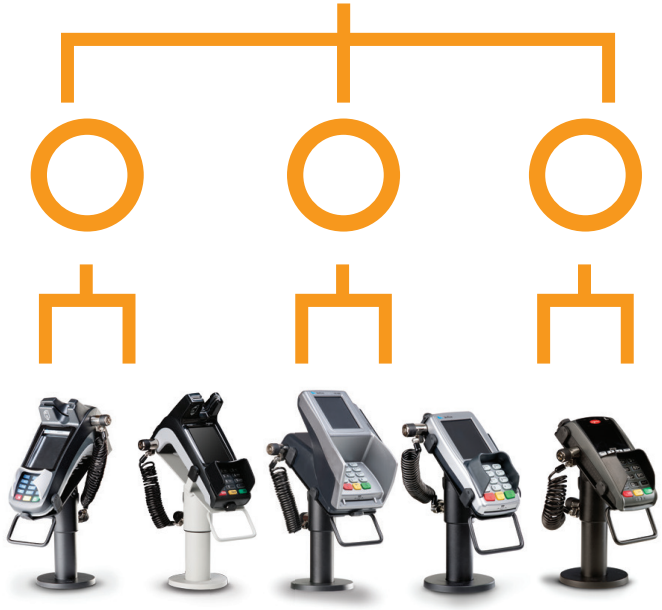
Lo skimming - l'acquisizione e il trasferimento non autorizzati dei dati di pagamento a un'altra fonte, a fini fraudolenti - è in aumento.

Lo skimming può assumere molte forme, dal shoulder surfing a frodi più sofisticate con lo scambio di terminali compromessi e dispositivi di ascolto NFC o Bluetooth®.



FATTO

Ci vogliono circa 30 secondi per rimuovere un terminale di pagamento e sostituirlo con un altro identico dotato di skimmer elettronici



NEMMENO FARLO MALE È UN'ALTERNATIVA PRATICABILE

Tentare di proteggere i dispositivi di pagamento con i prodotti che non sono progettati per lo scopo non fa altro che aggravare il problema, anziché risolverlo.

- Posizionamenti o montaggi mal concepiti compromettono l'esperienza del cliente
- Le apparecchiature mal progettate o non regolamentari spesso non sono conformi alla regolamentazione sulle disabilità e danno luogo a multe
- Le installazioni di scarsa qualità cedono e devono essere sostituite con conseguenti spese impreviste. Questo rallenta anche il pagamento alle casse, con conseguente calo delle vendite e scarsa fidelizzazione del cliente

Ottemperare a PCI DSS V3.0 Requisito 9.9

L'obiettivo di Ergonomic Solutions, sin da quando abbiamo iniziato a mettere in sicurezza i dispositivi nei negozi, è sempre stato di trovare un equilibrio fra la sicurezza dei pagamenti, il design, il costo totale di proprietà e l'accessibilità - sia per il personale sia per i clienti, sia normodotati che disabili.

È essenziale guardare con razionalità esattamente a quello che è necessario per raggiungere questo equilibrio, al fine di implementare la soluzione corretta con la tecnologia appropriata.

Quando si tratta di sicurezza dei dispositivi di pagamento, i retailer si trovano ad affrontare una crescente complessità del parco hardware in-store:

- **Sistemi POS tradizionali**
- **Sistemi POS modulari**
- **Dispositivi POS mobili**
- **Dispositivi tablet con collegamenti sia fissi che cablati ai dispositivi elettronici portatili**
- **Chioschi sia fissi che mobili con funzionalità di pagamento**
- **Dispositivi di pagamento sia di prima che di seconda generazione con scadenze incombenti per PCI V3.0**

La messa in sicurezza di un dispositivo terminale o mobile deve:

I retailer devono anche considerare la sicurezza di questi dispositivi dalla prima messa in servizio, attraverso la consegna e l'implementazione, la localizzazione, la messa in sicurezza e il funzionamento, fino alla manutenzione e, in definitiva, allo smaltimento.

Molti retailer hanno l'impressione, se un dispositivo è implementato nell'ambito di un programma di crittografia P2PE , che sia sicuro senza il bisogno di sicurezza fisica. Ebbene non è così. Il Requisito 9.9 si applica a tutti i dispositivi, come consigliato nel manuale di istruzioni P2PE.

Conformità PCI e quello che ciò significa per voi

Con i requisiti PCI che divengono sempre più rigorosi ed esigenti per le organizzazioni che ricevono i pagamenti, stiamo proponendo ai nostri clienti e partner consulenze su qualsiasi questione relativa al PCI attraverso il nostro PCI Professional Program.

La nostra enfasi è posta sulle consulenze sul PCI con un approccio facilmente comprensibile - per demistificare il PCI e aiutarvi con le domande che sorgono in sede di discussione e implementazione degli standard PCI al punto vendita. Il PCI è molto spesso oggetto di discussione per motivi di interpretazione. Il PCI è un insieme di pratiche di sicurezza essenziali che ogni organizzazione dovrebbe seguire e noi siamo a disposizione per guidare l'utente attraverso i numerosi standard sulla via che conduce a un POS sicuro e conforme.

Una violazione dei dati delle carte di pagamento può devastare una organizzazione e la sua clientela. I risultati di un incidente possono essere costosi, sia in termini finanziari sia di reputazione, di gran lunga più costosi rispetto a mettersi in regola con PCI DSS.

PCI Security Standards Council®
PARTICIPATING ORGANIZATION™

GLI ASPETTI PRATICI DELLA CONFORMITÀ PCI E DELLA SICUREZZA FISICA

Le soluzioni di pagamento SpacePole sono collaudate, solide e conformi a PCI V3.0 Requisito 9.9

- Prevenire il furto o la sostituzione con un terminale non autorizzato
- Prevenire l'acquisizione non autorizzata dei dati dall'infrastruttura di pagamento
- Prevenire l'aggiunta di apparecchiature per la strisciata al terminale o rete
- Proteggere i dati del PIN vulnerabili al shoulder surfing
- Proteggere i terminali incustoditi dalla rimozione fisica
- Proteggere non solo il terminale, ma anche i cavi

SpacePole® DuraTilt

Brevettato e collaudato in ambiente retail con la massima flessibilità e funzionalità

SpacePole® Low profile

Robusto, con rotazione dal cliente all'operatore

SpacePole® Light

Materiale composito ma con tutte le caratteristiche che è normale attendersi

SpacePole® SafeGuard M-Case

Per il commercio in movimento

Abbinate ai cavetti antifurto ClickSafe® di Kensington, nostro esclusivo partner per la sicurezza, e ai sigilli di sicurezza UV antimanomissione, le soluzioni di pagamento SpacePole vi permettono di stare tranquilli e proteggono la vostra reputazione ovunque esercitiate la vostra attività commerciale.

POSSIAMO AIUTARVI

Ergonomic Solutions

La società è il fornitore leader in Europa di soluzioni di pagamento attinenti la sicurezza fisica conformi alle migliori pratiche PCI e l'unica a proporre soluzioni di montaggio di tecnologia ad essere membro partecipante attivo del PCI Security Council.

Contattateci per sapere come Ergonomic Solutions possa sia aiutarvi a mettervi in regola sia fornirvi soluzioni di pagamento pronte per il Requisito 9.9.

Ergonomic Solutions International Ltd,
B1 Longmead Business Centre, Blenheim Road,
EPSOM KT19 9QQ, United Kingdom
Tel: +44 (0) 1372 728872
INSERT EMAIL
www.ergonomic-solutions.net/pci