SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

Come raggiungere la conformità PCI DSS semplificandosi la vita

Roma, 7 Giugno 2017

mediaservice.net
CORPORATE SECURITY & IMAGE

Relatori

Paolo SFERLAZZA

Senior Security Advisor

Resp. Div. Sicurezza Informazioni - @Mediaservice.net S.r.l.

Giusva FIUMANA

Direttore Sistemi - Passepartout S.p.A.

Massimiliano MONTERUMISI

Security Team Leader e Cloud Architect

Agenda

1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

@ Mediaservice.net in pillole

- Security Advisory company con sede a Torino e Roma
- Presente sul mercato dal 2000
- Servizi consulenziali strategici ed indipendenti
- Sicurezza Proattiva, Compliance, Governance, Formazione
- Sviluppo di metodologie e standard di sicurezza
- Partnership con istituti di ricerca internazionali
- Personale altamente qualificato e certificato

@ Mediaservice.net in pillole

@ Mediaservice.net è stata accreditata dal PCI Security Council in qualità di

- QSA Company (**Qualified Security Assessors**) da Ottobre 2009
- ASV Company **(Approved Scanning Vendor**) da Luglio 2011

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
APPROVED SCANNING VENDOR

@ Mediaservice.net, ha inoltre ritenuto di strategica importanza certificare e mantenere allineati la propria struttura e la competenza del proprio personale secondo le norme UNI EN ISO 9001 e ISO/IEC 27001 sull'ambito di:

"Progettazione ed erogazione di servizi di Advisory e formazione in materia di sicurezza delle informazioni".

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI
DNV·GL
ISO/IEC 27001

CERTIFICAZIONE DI SISTEMA QUALITÀ
DNV·GL
ISO 9001

mediaservice.net
CORPORATE SECURITY & IMAGE

5

Passepartout in pillole

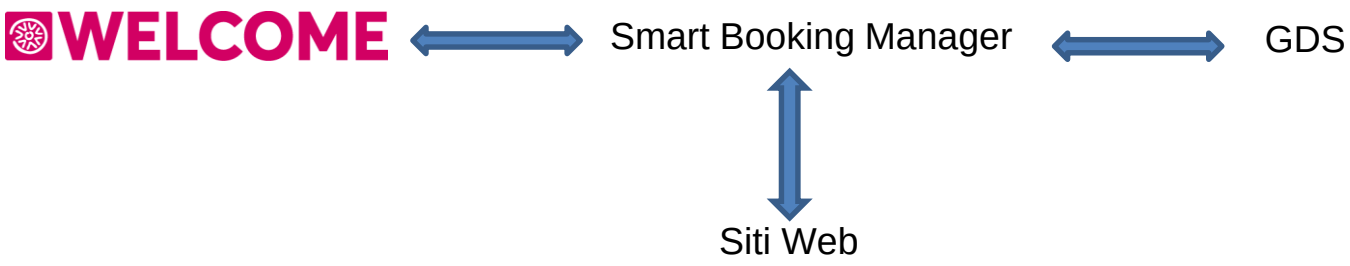
Passepartout nasce nel **1989** da un'idea ben chiara, creare una soluzione software per Piccole-Medie Imprese, semplice, affidabile e flessibile, capace di evolvere insieme alle esigenze dei clienti ed all'evoluzione del mercato.

Partendo dal mercato tradizionale delle PMI, negli anni Passepartout si è affermata anche quale produttore di soluzioni per commercialisti e nei settori dell'ospitalità, del benessere e della vendita al dettaglio, sviluppando prodotti specifici per Ristoranti, Hotel, Beauty Farm e Negozi.

Dal **2005** la Server Farm di Passepartout è iscritta presso il Registry Europe (RIPE), Autonomous System e Mantainer per la registrazione dei domini Internet.

Nel **2008** inizia ad offrire le proprie soluzioni software anche in modalità SaaS tramite la propria Server Farm.
Oggi offriamo soluzioni in ambiente CLOUD su più data center.

PASSCOM
MEXAL
PAGHE
RETAIL
WELCOME



Agenda

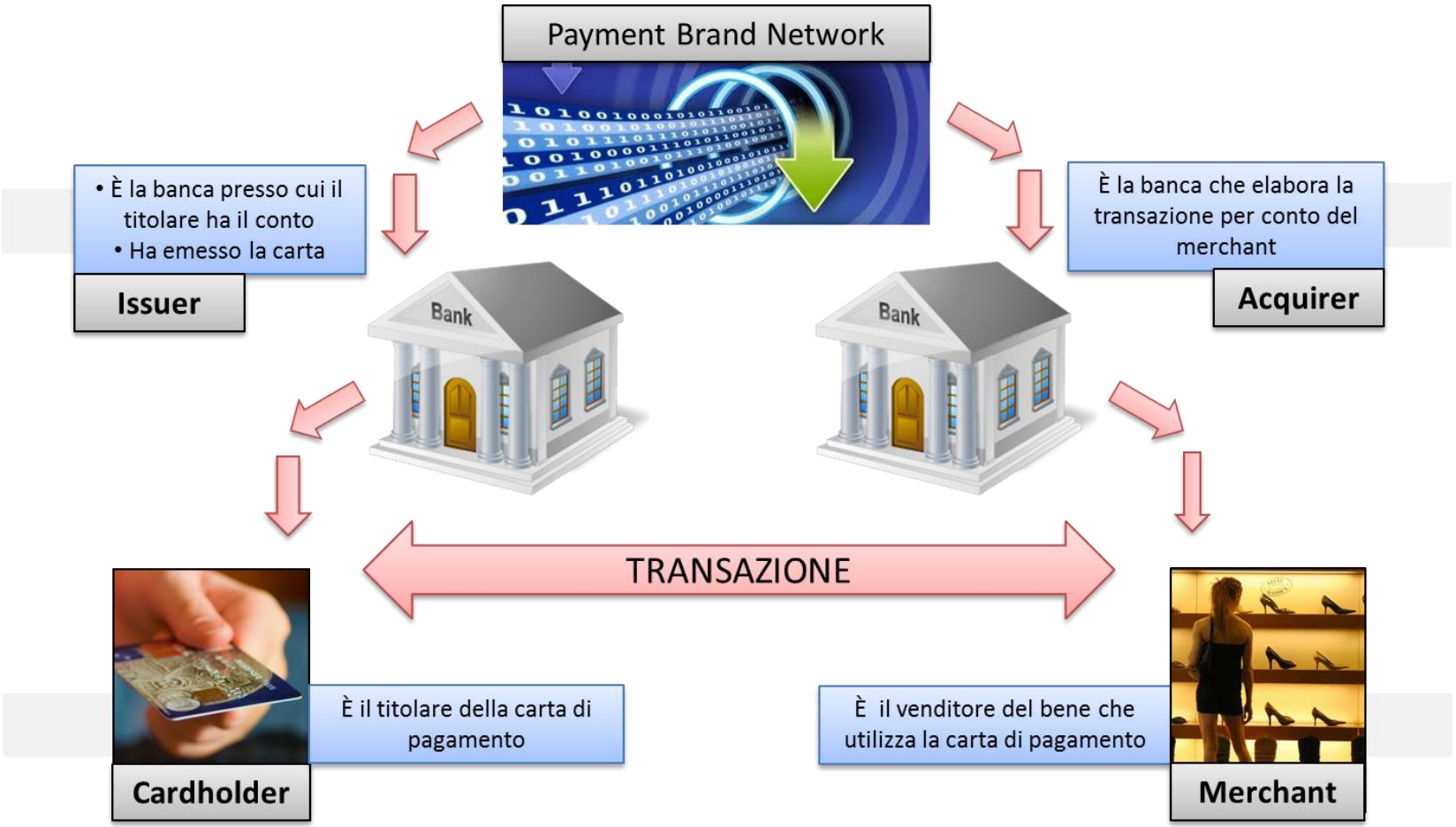
1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

PCI DSS (1)

Lo ***Standard PCI DSS*** è un insieme di *requisiti operativi e tecnici* per le organizzazioni che **accettano o che trattano** transazioni di pagamento.

Sviluppo e gestione di una rete sicura	1. Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta 2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati di titolari di carta	3. Proteggere i dati di titolari di carta memorizzati 4. Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche
Utilizzo di un programma per la gestione delle vulnerabilità	5. Utilizzare e aggiornare regolarmente il software o i programmi antivirus 6. Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	7. Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario 8. Assegnare un ID univoco a chiunque abbia accesso a un computer 9. Limitare l'accesso fisico ai dati dei titolari di carta
Monitoraggio e test delle reti regolari	10. Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta 11. Eseguire regolarmente test di sistemi e processi di protezione
Gestione di una politica di sicurezza delle informazioni	12. Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

PCI DSS (2)



PCI DSS (3)

Due tipi di transazioni con carte di pagamento

Card Not-Present

Una transazione fatta quando il *titolare della carta* ***non può*** *presentare fisicamente la carta* per un esame visivo da parte del commerciante al momento dell'ordine (e-commerce).

Card Present

Una transazione dove il *titolare della carta e la stessa sono presenti contemporaneamente al momento del pagamento*. Il pagamento viene finalizzato inserendo la scheda nel terminale POS (scheda con chip), o strisciata nell'apposito lettore del terminale (scheda solo con banda magnetica).

PCI DSS (4)

L'ambito di applicazione dei requisiti PCI DSS prevede che:
(cfr **Ambito dei requisiti PCI DSS - PCI DSS 3.2**)

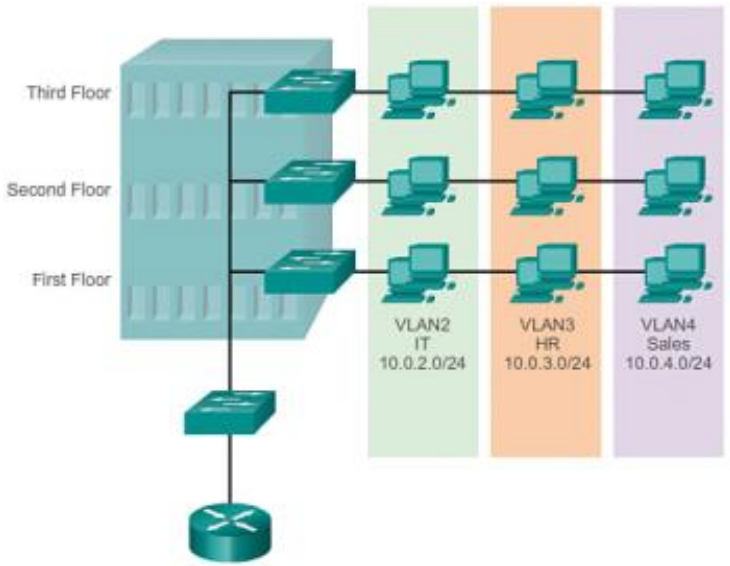
*"I requisiti di sicurezza PCI DSS siano applicabili a **tutti i componenti di sistema** inclusi nell'ambiente dei dati dei titolari di carta o collegati ad esso."*

*"L'ambiente dei dati dei titolari di carta sia **composto da persone, processi e tecnologie che memorizzano, elaborano o trasmettono** i dati dei titolari di carta o i dati sensibili di autenticazione."*

*"I **componenti di sistema** includano dispositivi di rete, server, dispositivi informatici e applicazioni."*

PCI DSS (5)

Lo stesso standard prevede l'utilizzo della segmentazione per ridurre lo scope (cfr **Segmentazione di rete - PCI DSS 3.2**)



La segmentazione di rete ***non costituisce un requisito PCI DSS*** *tuttavia, è un metodo consigliato che* ***consente di ridurre****:*

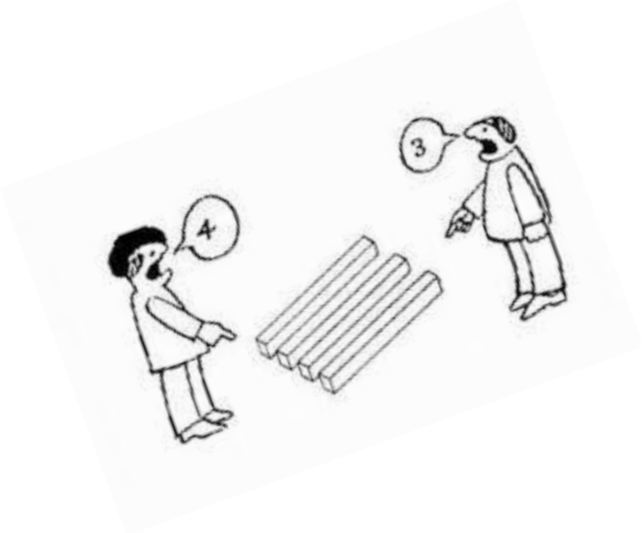
- ***l'ambito*** *della valutazione PCI DSS;*
- ***il costo*** *della valutazione PCI DSS;*
- *il costo e* ***la difficoltà*** *dell'implementazione e della gestione dei controlli PCI DSS;*
- ***i rischi*** *per un'organizzazione (grazie al consolidamento dei dati dei titolari di carta in un minor numero di posizioni controllate).*

Senza un'adeguata segmentazione ***l'intera rete rientra nell'ambito PCI DSS****.*

PCI DSS – Il punto di vista del Cliente

*PCI DSS dal punto di vista dei **clienti***

- Lunghi tempi di implementazione
- Alti costi di implementazione per l'azienda
- Forte effort nelle attività di processo e/o documentale
- Forte effort nelle attività tecnologiche
- Difficoltà nell'identificazione del perimetro
- Difficoltà nell'allocazione risorse



PCI DSS – Il punto di vista del QSA

PCI DSS dal punto di vista del QSA

- Validare con precisione il perimetro dell'assessment
- Individuare tutte le posizioni ed i flussi dei dati dei titolari di carta ed assicurare che siano state incluse nell'ambito PCI DSS
- Confermare che l'ambito della valutazione sia definito e documentato con accuratezza.
- Verificare tutti i controlli implementati affinché ottemperino a quanto prescritto dallo standard

PCI DSS – Il punto di vista del QSA

PCI DSS dal punto di vista del QSA

- Dati delle carte di credito **inviate via email** (es riservazioni alberghiere)
- Non vengono mai considerati in scope sistemi che non trattano dati delle carte di pagamento attestati sulle reti ove avvengono transazioni
- SaQ compilati dando per scontata la conformità a tutti i requisiti (anche quelli non applicabili allo specifico contesto)
- Difficolta nell'identificazione tra Merchant e Service Provider e definizione del livello di appartenenza e quindi il SaQ che è necessario adottare
- Dati delle carte **salvati in chiaro** (file excel su share di rete)

Agenda

1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

Riduzione Scope

Per restringere l'ambito di applicabilità della PCI DSS, è possibile **ridurre il numero di componenti di sistema** che sono inclusi o sono collegati al *Card Data Environment (CDE)*.

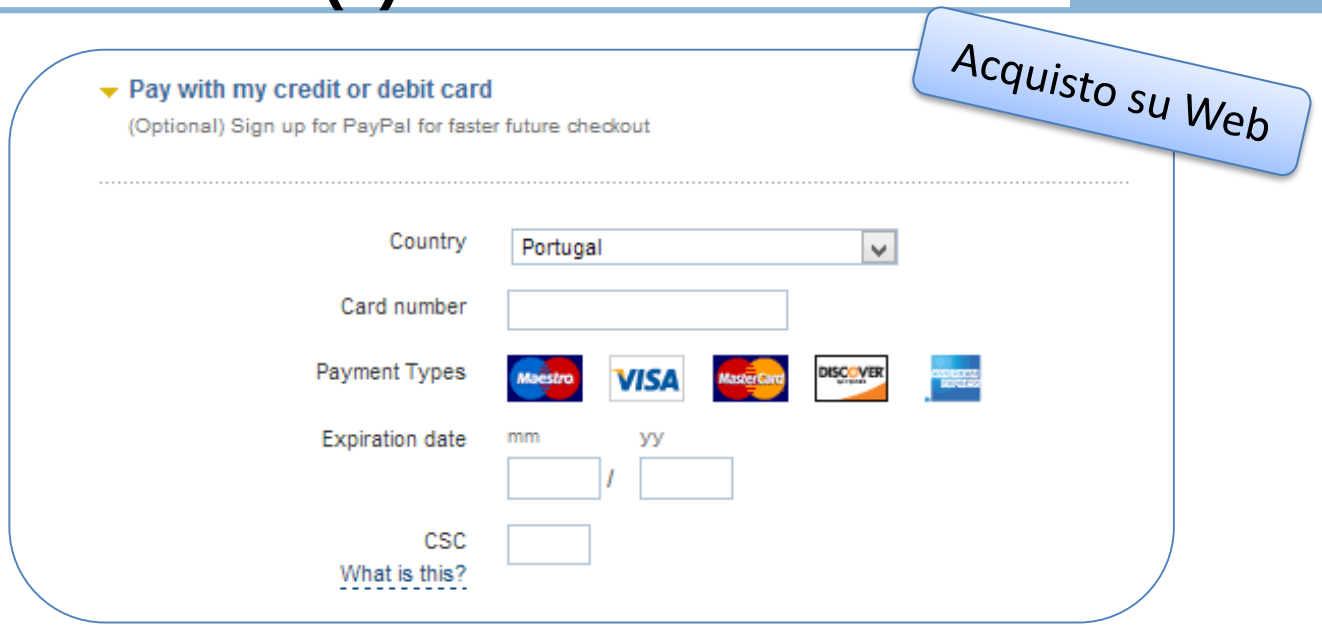
Per fare questo è possibile adottare alcuni accorgimenti:

- Segmentare la rete creando un ambiente dedicato PCI
- Soluzioni P2PE (Point to Point Encryption)
- Soluzioni PA-DSS
- Tokenizzazione
- Servizi mediante Service Provider certificati PCI DSS

Agenda

1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

Card not-Present (1)



- **Spesso i dati** vengono **salvati in modo non sicuro**
- **Spesso i dati** vengono **inviati in modo non sicuro** (es. via email)
- Il **salvataggio** dei dati delle carte di pagamento **incrementano** l'effort per il raggiungimento della conformità
- Le **contromisure** da implementare per il salvataggio dei dati delle carte di pagamento sono diverse e spesso di **complessità elevata**.

CERTIFICAZIONE PCI DSS
WELCOME SMART BOOKING MANAGER

The challenge (1/4)

«I locali, gli uffici, le postazioni di lavoro afferenti al CDE e tutte le risorse fisiche rese disponibili ai dipendenti, che operano a vario titolo sui sistemi che gestiscono i dati delle carte di pagamento devono essere utilizzati e protetti con la massima diligenza, al fine di garantire un'efficiente conduzione dell'attività lavorativa ed il prevenire di eventi che possano andare ad incidere sulla sicurezza delle informazioni, con particolare riferimento ai dati delle carte di pagamento.»

Check List PCI 3.2

534 punti da soddisfare!!

The challenge (2/4)

Firewall NOC

WAF Redundancy

UPS

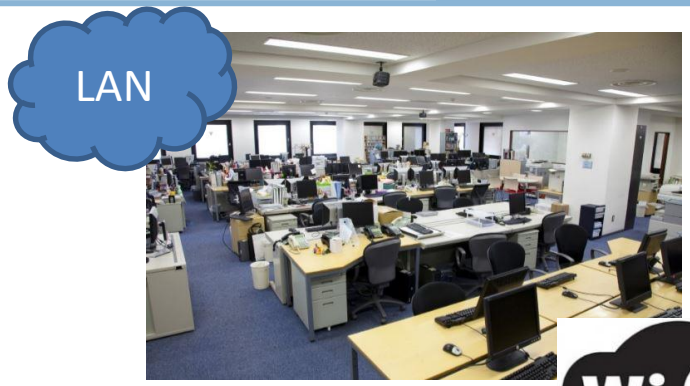
Gruppo Elettrogeno

Antincendio

Videosorveglianza

SUPERSICURO!

Ma è certificato PCI DSS?



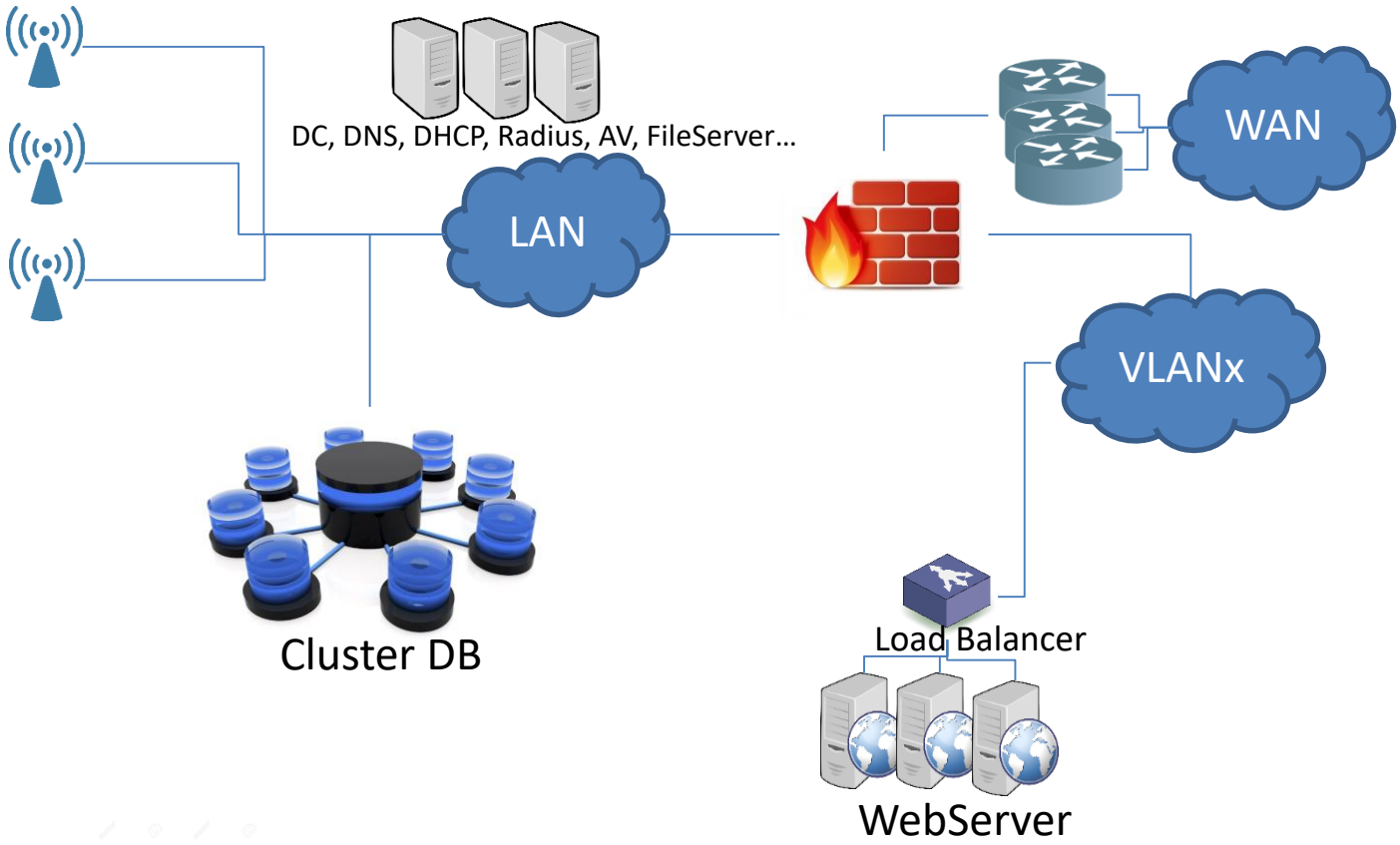
Cluster DB

No firewall

E il SIEM di tutta l'architettura?

mediaservice.net
CORPORATE SECURITY & IMAGE

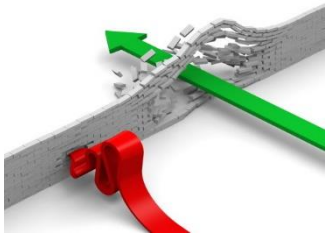
The challenge (3/4)



Non è compliant!

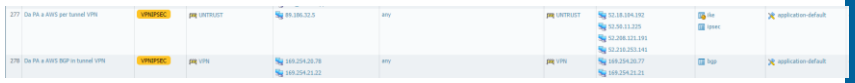
…E anche se lo fosse è complesso e costoso da mantenere compliance.

The challenge (4/4)



Verifica trimestrale delle firewall rules

Quante rules ci sono?



…quasi 300

Vulnerability Assessment Interno

- Trimestrale
- Perimetro molto vasto

Non è compliant!

…E anche se lo fosse è complesso, costoso da mantenere compliance.

Adottare un processo formale di approvazione e di controllo delle connessioni di rete e dei cambiamenti delle configurazioni dei firewall e dei router.

Ingessare l'operatività quotidiana
Rischio di errori!

The solution (1/3)

Spostare il perimetro in un'infrastruttura già PCI DSS Compliant

Creare un'infrastruttura sicura, e facilmente controllabile

Creare un'infrastruttura scale-out

Automatizzare tutti i processi di deploy

Ridurre al minimo le modifiche, specialmente quelle manuali!

The solution (2/3)

PCI Security Standards Council

PCI DSS Cloud Computing Guidelines

Figure 3: Example of how PCI DSS responsibilities may be shared between clients and CSPs.

	Client
	CSP
	BOTH Client and CSP

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

The solution (3/3)

HEADQUARTER

Log analisys procedure

Log repo services

VPN

- permit to cloud only few port
- BGP over VPN for failover

INTERNET

Cluster DB dedicato

Deploy service

CHEF

VPN End-Point

Web Server

L3 FWs

Web Server

Load Balancer

PAN Repository Encrypted Services

L3 FW

WAF

Perimetro PCI DSS

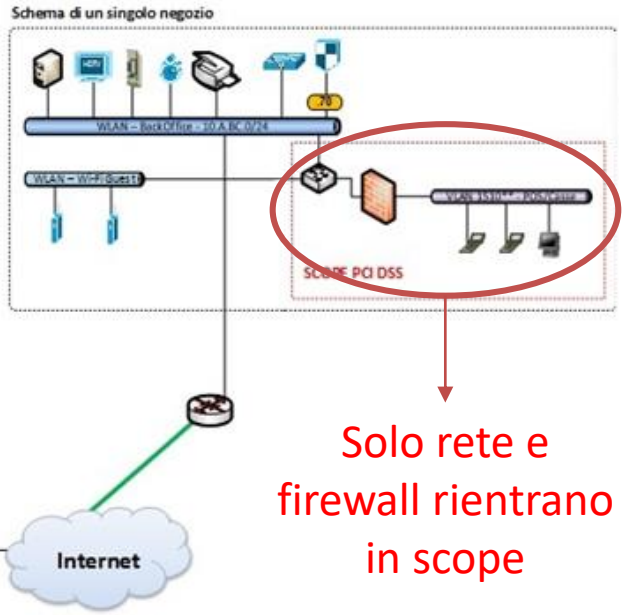
Agenda

1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

Card Present

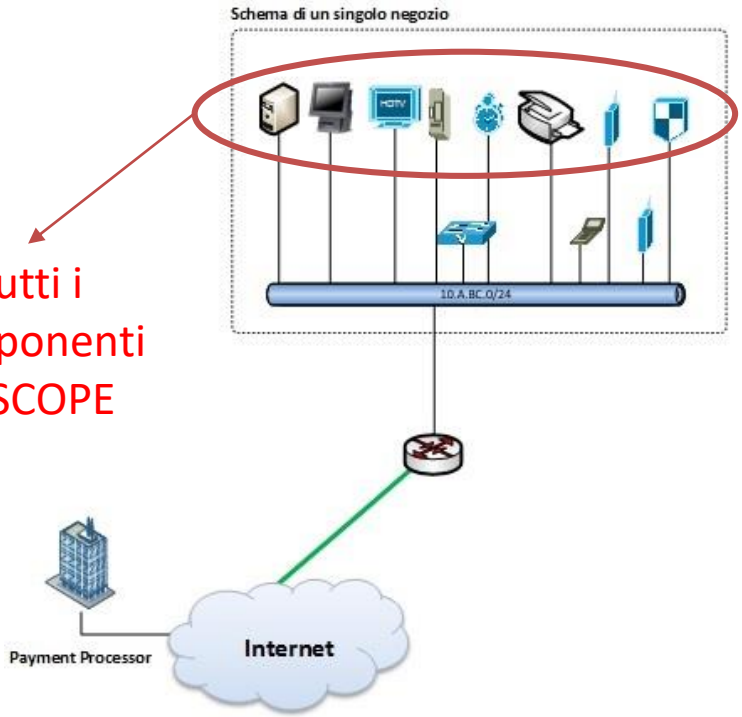
… prendiamo il caso di una catena di negozi

Questi rientrano in PCI DSS in quanto **trattano i dati** della carte di pagamento utilizzate **fisicamente** durante l'acquisto di beni



Solo rete e firewall rientrano in scope

Tutti i componenti in SCOPE



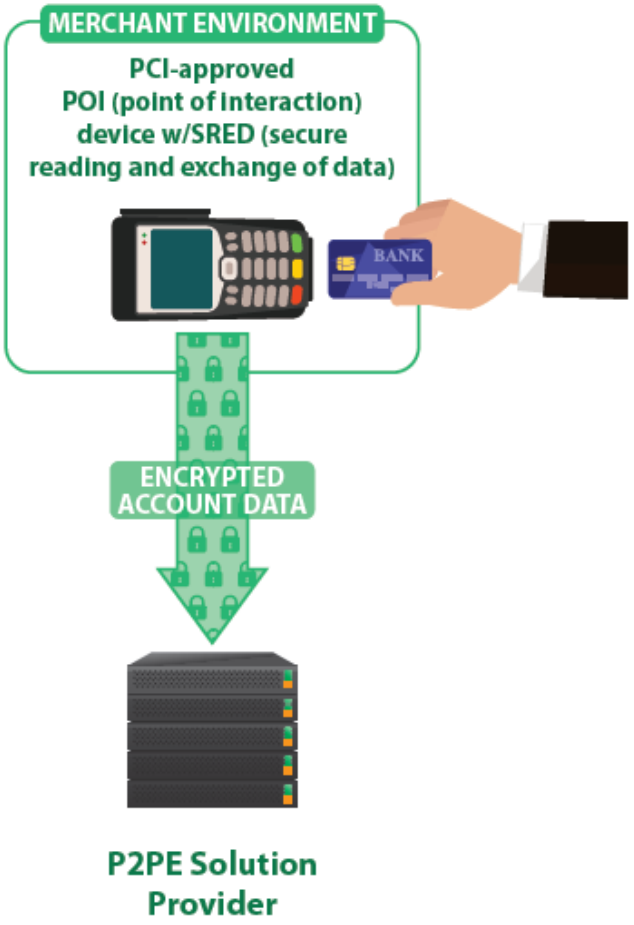
Senza adeguata segmentazione tutti i componenti di rete attestati sulla rete dei POS rientrano nel perimetro PCI DSS

Cos'è P2PE

…se risulta difficile installare e gestire una rete segmentata si può adottare una soluzione P2PE!

È una soluzione fornita da un Service Provider validato da PCI SSC che sfrutta una combinazione di dispositivi, applicazioni e processi sicuri che permettono di crittografare i dati di carta dei titolari direttamente al dispositivo PTS-POI ed inviarli nell'ambiente sicuro di decifratura del Service Provider.

Quest'ultimo, dal proprio ambiente sicuro, gestisce la trasmissione dei dati di carta all'Acquirer per completare la transazione.



Agenda

1. Introduzione
2. Lo Standard PCI DSS
3. … la riduzione dello Scope
4. Case History Card not-present
5. Una possibile soluzione per sistemi Card Present
6. Conclusioni

….per concludere

PCI DSS è uno standard ***complesso***

… ma si può ***semplificare***.

È necessario trovare il **giusto compromesso** tra costi e benefici, me è da tenere a mente che **esistono soluzioni** che permettono un raggiungimento della conformità in modo più **agevole**.

Per qualsiasi approfondimento e confronto sul tema siamo a disposizione:

pci@mediaservice.net

Domande?