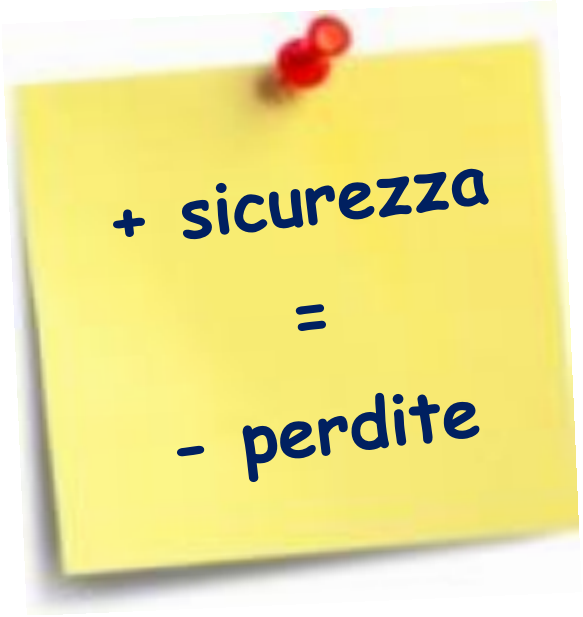
Security Verification Standard Framework BANCOMAT®

Veronica Borgogna
Consorzio BANCOMAT®

L’assioma della sicurezza



Le perdite derivano da <u>eventi dannosi</u>, ossia fenomeni indesiderati – accidentali o volontari – che compromettono il corretto funzionamento del sistema nelle sue varie componenti.

Incidenti	**Generano delle perdite**
Attacchi deliberati	**Causano da una parte delle perdite e dall’altra generano dei “profitti”.**

Nel mondo dei sistemi di pagamento con carte l’appetibilità del guadagno tende a sbilanciare il peso verso l’accadimento di attacchi deliberati.

Attacchi tipici agli schemi di pagamento

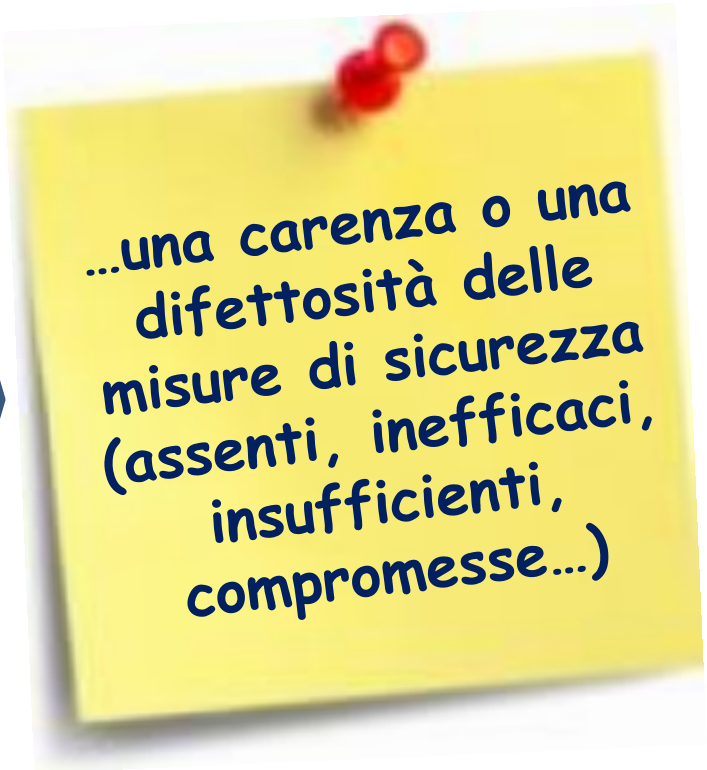
ATTACCHI FISICI	**Cattura carta (*card trapping*)**	Cattura della carta mediante l'inserimento di un elemento all'interno della feritoia dell'ATM. Tale frode è associata in genere a tecniche volte all'identificazione del PIN
	Cattura banconote (o *cash trapping*)	Inserimento di elementi artigianali nello *shutter* volti a compromettere l'erogazione delle banconote
ATTACCHI LOGICI	**Skimming/ shimming**	Attraverso l'installazione di *device* capaci di leggere i dati delle carte operanti con tecnologia a banda (*skimmer*) e di memorizzarli/ inviarli a supporti esterni, vengono riprodotte delle carte con la sola traccia magnetica in grado di lavorare su terminali con questa tecnologia
	Malwering	Attraverso un'infezione di tipo malware che può attuarsi secondo diverse modalità, il dispositivo è posto sotto il controllo dei frodatori che vanno alla ricerca di informazioni sensibili quali dati identificativi del *card holder* o PAN delle carte
	Riconfigura-zione dei dati della traccia magnetica	Alcune carte rubate vengono alterate nelle caratteristiche di funzionamento della traccia magnetica al fine di modificarne la natura e bypassando l'operatività a chip

Vulnerabilità e minacce

Qualsiasi tipologia di attacco osservata, tuttavia, si basa sulla

scoperta di una vulnerabilità – hardware, software, normativa, organizzativa, di processo – e sulla capacità di sfruttarla per trarne un vantaggio illecito.

La vulnerabilità si definisce quindi come…



E’ fondamentale individuare le vulnerabilità insite nel nostro sistema prima che siano **sfruttate da altri a scopo fraudolento**.

When, where, how

Le vulnerabilità sfruttano il momento o il luogo dell'interazione e rappresentano l'occasione d'attacco.

- **Cattura carta (*card trapping*)**
- **Cattura banconote (o *cash trapping*)**
- **Skimming/ shimming**
- **Malwering**
- **Riconfigurazione dei dati della traccia magnetica**

- ✓ Il **card reader** dell'ATM/ POS
- ✓ La **fascia** dell'ATM
- ✓ La traccia **magnetica** della carta

- ✓ La linea di comunicazione tra il PC dell'ATM e l'unità del **dispenser**
- ✓ La linea di comunicazione tra il PC dell'ATM e le **periferiche** (porte USB, tastiere esterne, unità CD/ DVD)
- ✓ La linea di comunicazione tra il PC dell'ATM e **l'host**

Il modello di sicurezza

Un framework di sicurezza si compone di vari step.

1° STEP

La prima fase è quella del *risk profiling*, che ha come scopo l'individuazione dei possibili rischi in gioco.

ESEMPIO: lettura dei dati di una carta di pagamento

2° STEP

La seconda fase è la comprensione dei possibili scenari e delle minacce ad essi collegati

ESEMPIO: cattura dei dati mentre è in corso una transazione web (scenario); attacco *man-in-the-middle* (minaccia)

3° STEP

La fase finale misura la capacità di resistere agli attacchi in quanto è volta a rintracciare le «falle» del sistema di sicurezza che hanno permesso la realizza-zione dell'attacco

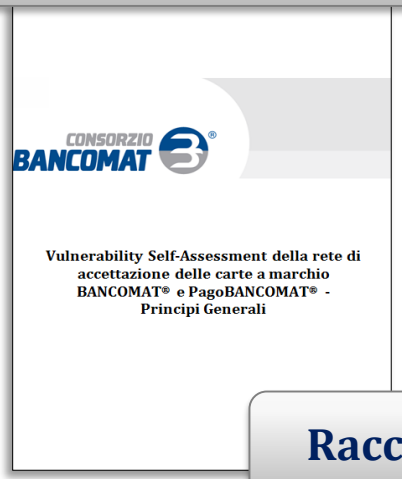
ESEMPIO: antivirus inefficace

Security Verification Standard Framework

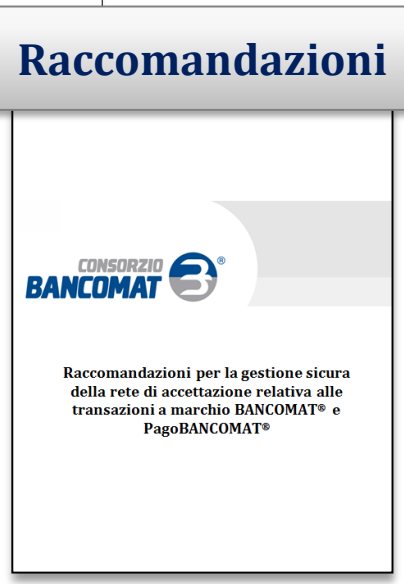
A tale scopo, a fronte dei risultati ottenuti dagli assessment condotti negli anni precedenti, il Consorzio ha svolto un progetto volto a definire un **framework di sicurezza** formato da:

- requisiti per il rafforzamento dei presidi di sicurezza antifrode,
- best practice per l'espletamento dei processi,
- elementi specifici di controllo e verifica – a livello organizzativo, tecnologico e di processo

Principi per il rafforzamento della sicurezza antifrode



Raccomandazioni



OBIETTIVO FINALE

Rilevare delle vulnerabilità e mettere in atto interventi di mitigazione per rafforzare il livello di sicurezza della rete di accettazione.

Perimetro dello Standard

Campo di applicazione

Specifiche tecnico/ funzionali ≠ **Principi per il rafforzamento della sicurezza antifrode**

Contengono elementi di sicurezza insiti nel protocollo.

ESEMPIO: SPED/DEF 41 (Specifiche di sicurezza per i terminali POS); SPE/DEF 50 (Requisiti di sicurezza del processo di Issuing).

Coprono un perimetro più ampio che va oltre quello di omologazione. Contengono requisiti per la messa in sicurezza degli aspetti organizzativi, procedurali, logistici.

ESEMPIO: elementi per messa in sicurezza di:

- **servizi di installazione terminali**
- **servizi di manutenzione componenti hardware**
- **servizi di sviluppo software**

Soluzioni di sicurezza per gli accessi logici

Soluzioni di sicurezza della rete

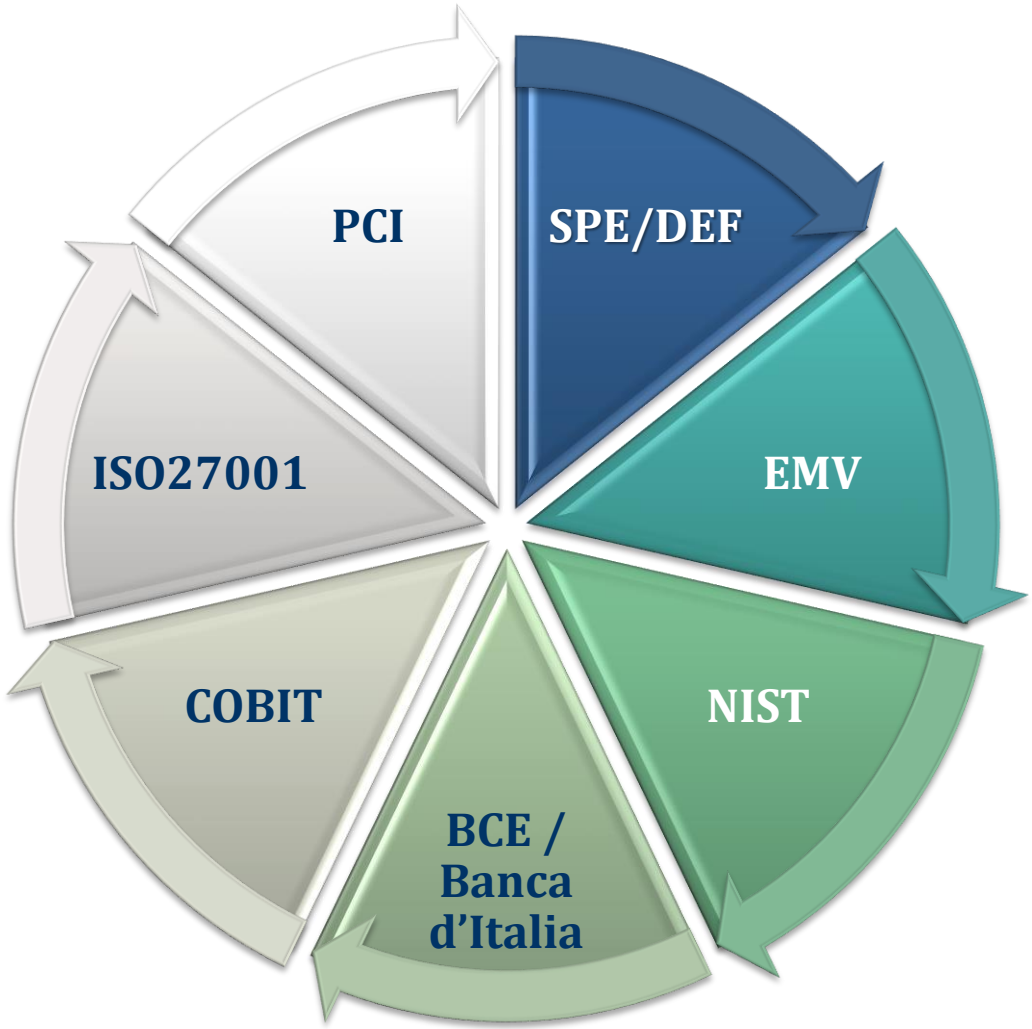
Soluzioni per la gestione della crittografia

Soluzioni per il monitoraggio / logging

Soluzioni di Business Continuity Management e Disaster recovery

Basi normative

La definizione dello Standard si è basata su un'analisi delle normative, degli standard internazionali e delle best practice applicabili ai diversi ambiti di analisi, funzionali ad una significativa ed efficace identificazione delle aree di controllo per l'individuazione delle vulnerabilità cui le banche sono esposte.



AMBITI DI ANALISI

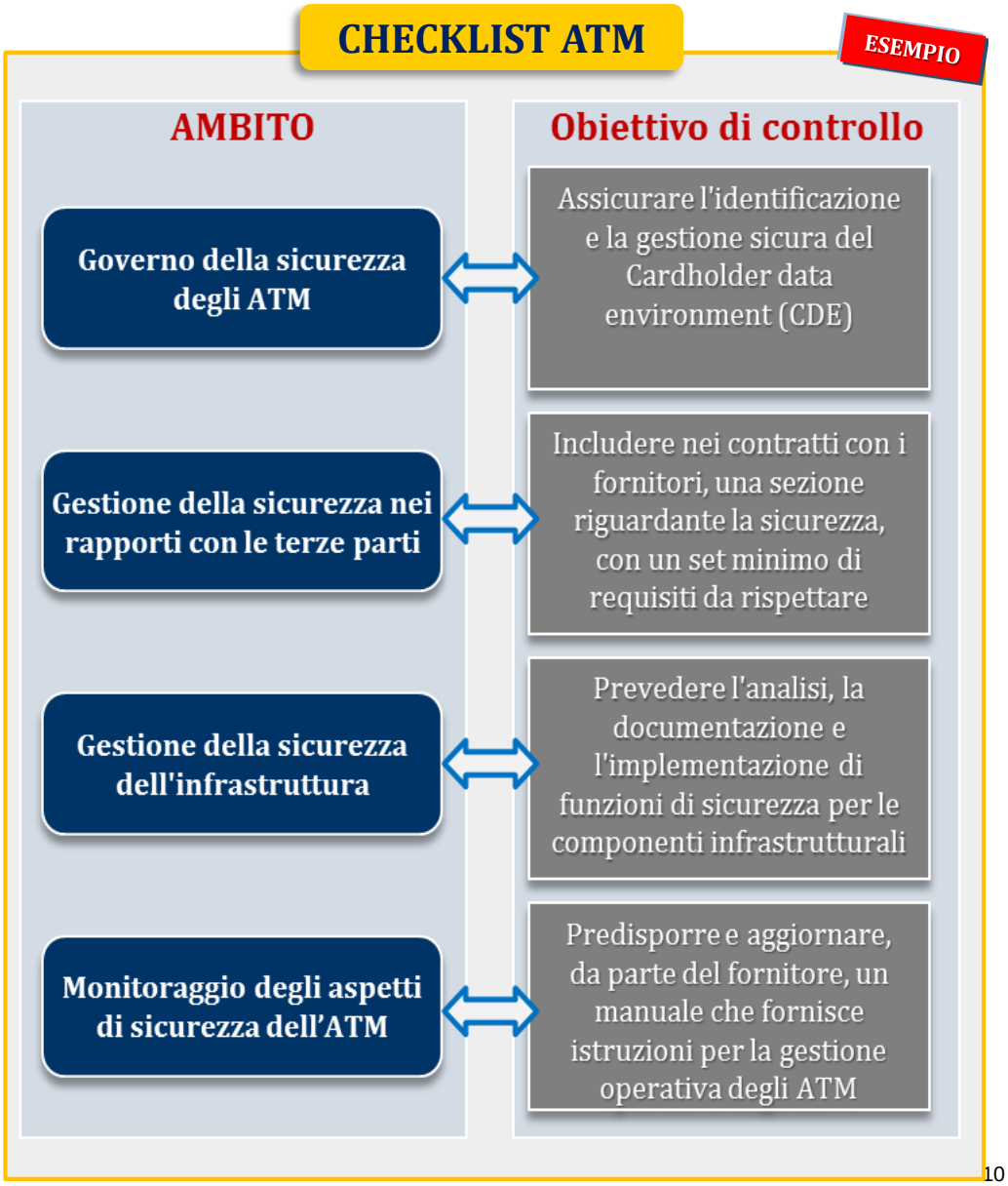
- Autorizzativo
- ATM
- Gestore Terminali
- Certification Authority
- POS

Processo di Vulnerability Self-Assessment

Il processo di *vulnerability self-assessment* è il processo di ricognizione finalizzato all'identificazione delle vulnerabilità tecniche, di processo e organizzative che potrebbero determinare rischi per la sicurezza, se sfruttate per realizzare eventuali attacchi.

CHECKLIST DI CONTROLLO

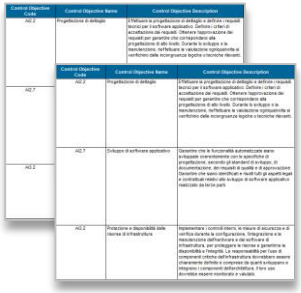
E' lo strumento con il quale si realizza il processo di self-assessment. All'interno della checklist, specifica per ogni ambito analizzato (es. ATM, POS, Gestore terminali etc.), in corrispondenza di ciascun ambito di sicurezza vengono definiti i controlli più efficaci per il contesto di riferimento.



Come si svolge l'assessment?

Consorzio BANCOMAT®

...il Consorzio stabilisce modi e tempi di avvio del *self-assessment*...



Aderenti

Gli Aderenti individuano all'interno dell'organizzazione le strutture preposte ai diversi ambiti...

... compilano la/e checklist...

Consorzio BANCOMAT®

Sulla base dei risultati, il Consorzio può:

- ***proporre miglioramenti agli Aderenti***
- ***modificare SPE/DEF e/o pubblicare nuovi standard***
- ***Intervenire per il rafforzamento delle difese***

La sicurezza è l'abilità di evolvere

L'obiettivo finale del nostro nuovo framework è quello di preservare l'autonomia nell'offerta dei servizi di mercato (customizzazione) portando però tutti gli operatori allo stesso livello di sicurezza, pur nella complessità della catena di erogazione attraverso un irrobustimento dello standard.

Se ieri il Consorzio profilava rischi e suggeriva strategie, oggi guida il sistema verso le condotte più opportune.

Grazie