VARNOST KARTIČNEGA POSLOVANJA

PCI DSS
Paymet Card Industry
Data Security Standard

Alenka Glas
Svetovalka za področje varnosti
FMC d.o.o.

FMC Group

FMC
FMC Group

Predstavitev predavateljice

FMC d.o.o., Svetovalka za področje varnosti

Vodilni presojevalec (lead auditor):

- ISO/IEC 27001 – Sistem vodenja varovanja informacij
- BS 25999 – Sistem vodenja neprekinjenega poslovanja

Ostala področja svetovanja:

- PCI DSS
- ZVDAGA
- Upravljanje revizijskih sledi
- ….

FMC Group

FMC
FMC Group

Skupina FMC Group

FMC Group

- FMC d.o.o. – celovite rešitve
- PRO Servis d.o.o. – zanesljiv IT servis
- Miška d.o.o. – izobraževanje po meri
- iStore – trgovina v City parku
- SO-CE d.o.o. – trgovina v City parku
- Skupina FMC d.o.o. – skupne služne

Vsebina

Predstavitev PCI DSS, PCI SSC

Kaj je pri kartičnem poslovanju potrebno varovati

Kako uvajati PCI DSS

Učinkovitost PCI DSS

FMC Group

FMC
FMC Group

Varovanje podatkov

Podatki o kartičnih računih so zaželena tarča kriminalcev.

Pred napadi se je mogoče zaščititi na različne načine (varnostni standardi), uspešno dobro prakso pa predstavljajo standardi iz družine PCI.

Elektronsko poslovanje je omogočilo nove poslovne poti, ki se zanašajo na učinkovit program za varovanje informacij, s katerim si lahko podjetje pridobi zaupanje strank...

FMC
FMC Group

PCI DSS

Standard upravlja organizacija Payment Card Industry Security Standards Council (PCI SSC), ki so ga ustanovili:

- **MasterCard**
- **Visa Card**
- **American Express**
- **DiscoverCard**
- **JCB International**

FMC Group

FMC
FMC Group

PCI standardi

- **PCI DSS – Payment Card Industry Data Security Standard**
  - **PCI DSS verzija 1.0 (januar 2005)**
  - **PCI DSS verzija 1.1 (september 2006)**
  - **PCI DSS verzija 1.2 (oktober 2008)**
  - **PCI DSS verzija 2.0 (oktober 2010)**
- PCI PA DSS – Payment Application Data Security Standard
- PCI PTS – PIN Transaction (PTS) Security Requirements

FMC
FMC Group

Nastanek PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) je namenjen varovanju informacij o karticah in njihovih imetnikih

Osnova so varnostni standardi nosilcev kartičnih produktov:

- MasterCard – Site Data Protection
- Visa Card – Information Security Program
- American Express – Data Security Operating Policy
- Discover – Information and Compliance
- JCB – Data Security Program

PCI DSS standard povzema kontrole iz standarda ISO/IEC 27002 in jih dopolnjuje s specifični kartičnimi zahtevami.

FMC
FMC Group

PCI DSS skladnost – za koga velja

PCI DSS postavlja okvire varnega kartičnega poslovanja in je obvezen za vse, ki

zajemajo, obdelujejo, hranijo ali posredujejo podatke o plačilnih karticah in njihovih imetnikih

- Procesni centri
- Prodajna mesta
- Banke podpisnice pogodb s prodajnimi mesti (acquirer)
- Banke izdajateljice kartic (issuer)

FMC Group

FMC
FMC Group

Definicija PCI DSS

PCI DSS je odprt standard:

- združuje tehnične in poslovne zahteve za vse organizaciie. ki zaiemaio. obdeluieio. hranijo ali posre n njihov
- je glo pobudo vodilr
- name

PCI Security Standards Council

PCI DSS Requirements	Testing Procedures	In Place	Not in Place
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	**12.6.a** Verify the existence of a formal security awareness program for all employees.		
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:		
12.6.1 Educate employees upon hire and at least annually.	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, memos, web based training, meetings, and promotions).		
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually.		
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.	**12.6.2** Verify that the security awareness program requires employees to acknowledge (for example, in writing or electronically) at least annually that they have read and understand the company's information security policy.		

Zakaj uvajati PCI DSS

PCI DSS pomeni omejevanje tveganj in poskuša zagotoviti:

- varno poslovanje s plačilnimi karticami za imetnike k
- varno pos ami za trgovce,
- izogibanje
- izogibanje a,
- skladnost z zakonodajo in regulativo.

FMC Group

FMC
FMC Group

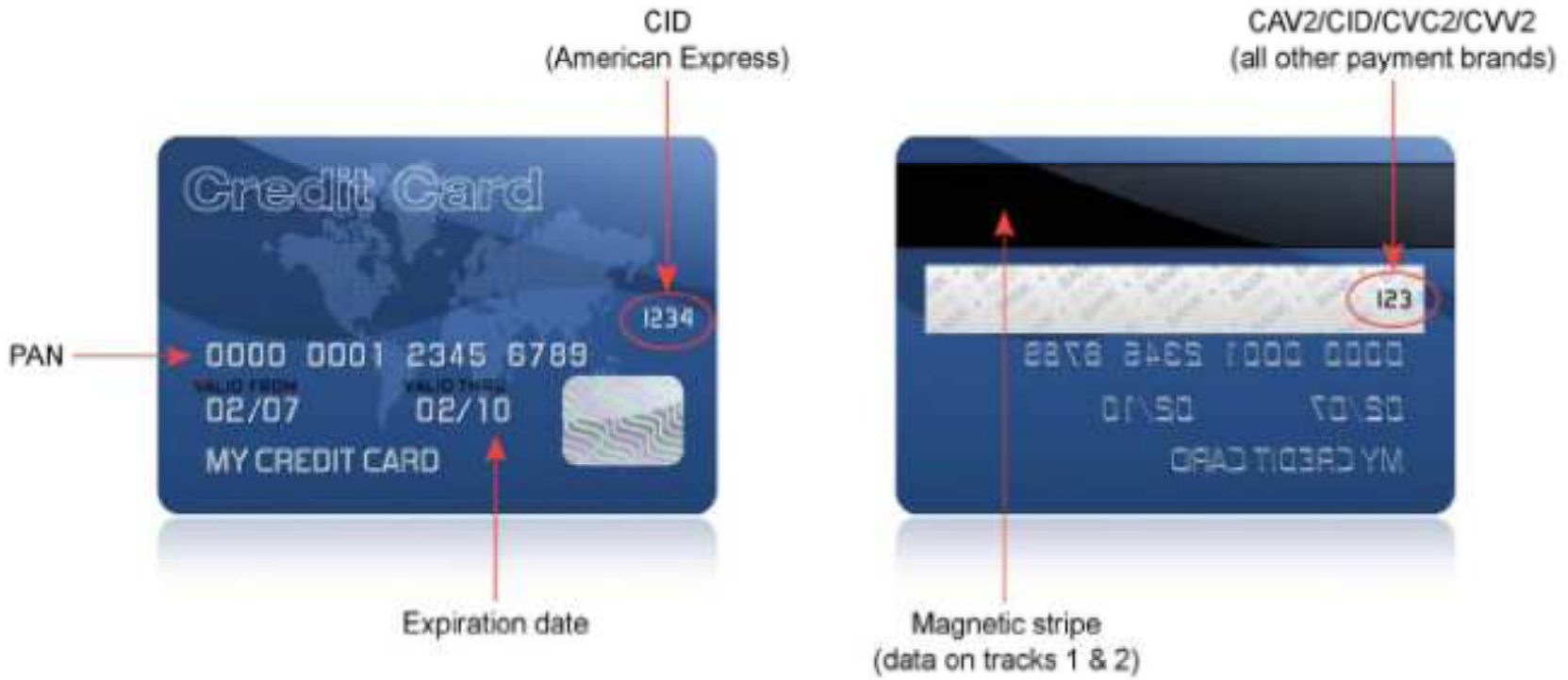
Kaj je po standardu potrebno varovati

	Vrsta podatka	Shranjevanje	Zahtevana zaščita	Kriptiranje podatkov
Podatki o plačilni kartici	Številka kartice PAN	Da	Da	Da
	Imetnikovo ime	Da	Da	Ne
	Servis koda	Da	Da	Ne
	Datum veljavnosti	Da	Da	Ne
Občutljivi podatki za odobritev plačila	Celoten magnetni zapis	Ne	N/A	N/A
	CAV2 / CVC2 / CVV2 / CID	Ne	N/A	N/A
	PIN / PIN blok	Ne	N/A	N/A

FMC Group

FMC
FMC Group

Podatki, ki so predmet varovanja



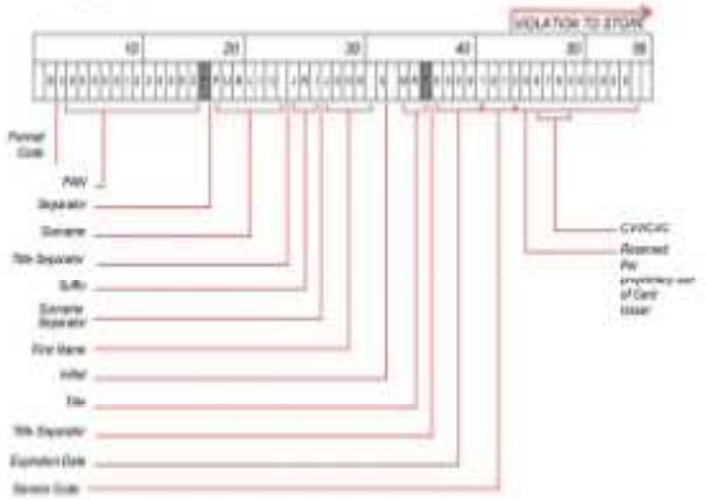
FMC Group

FMC
FMC Group

Podatki, ki so predmet varovanja

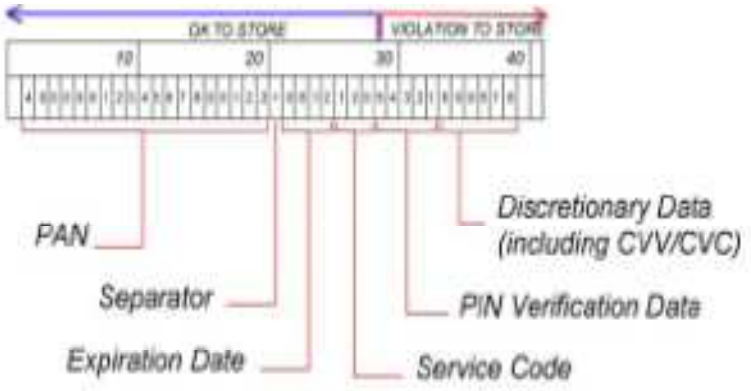
Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters



Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters



FMC Group

FMC
FMC Group

Struktura standarda

- 6 področij
- 12 zahtev
- podzahteve

FMC Group

FMC
FMC Group

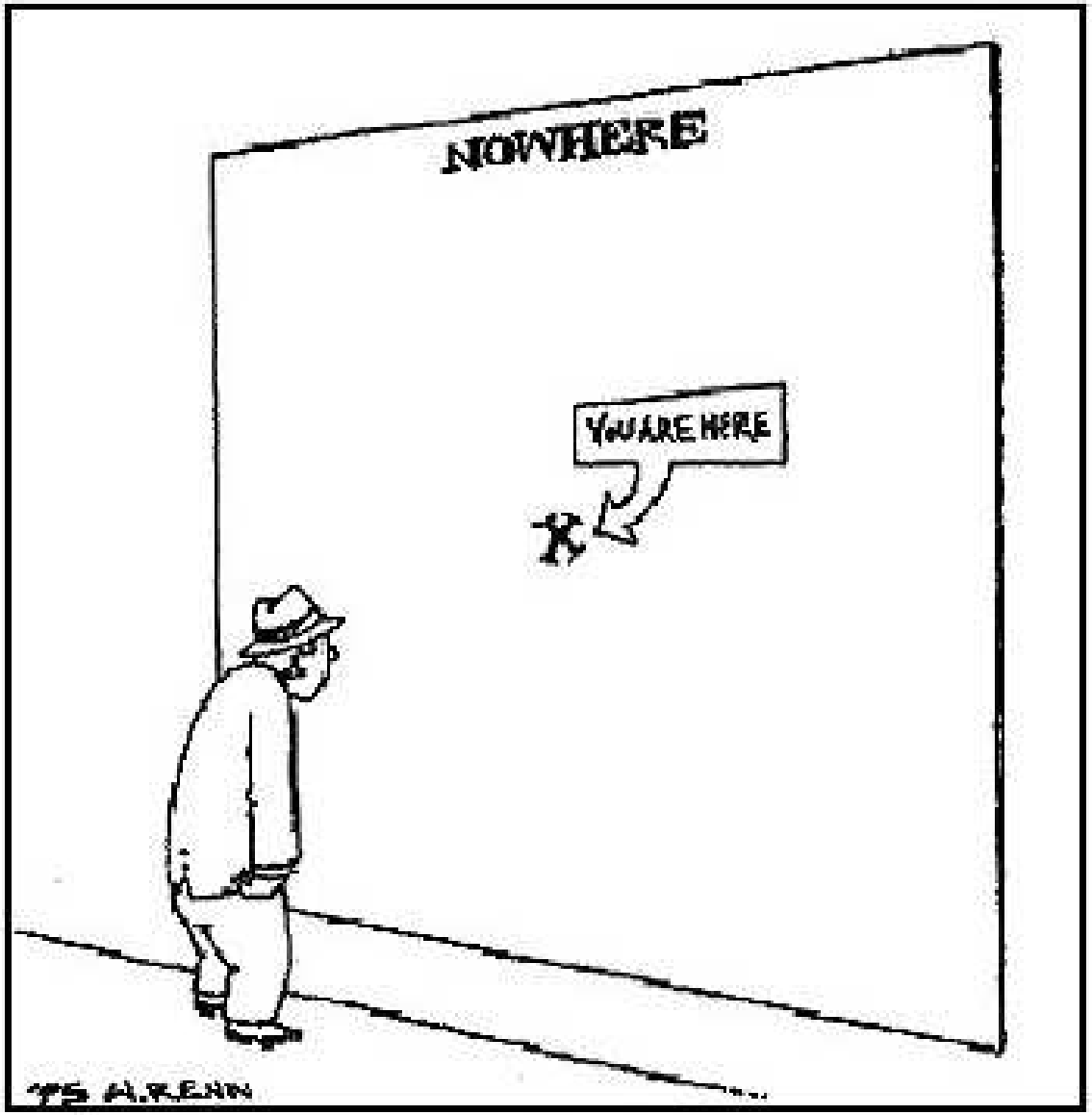
Področje	PCI DSS Zahteva
Vzpostavitev in vzdrževanje varnega omrežja	1 – Vzpostaviti in vzdrževati konfiguracijo požarne pregrade 2 – Ne uporabljati privzetih nastavitev, ki jih dobavi prodajalec sistema, za sistemska gesla in druge varnostne parametre
Varovanje podatkov o imetniku plačilne kartice	3 – Zavarovati shranjene podatke o imetniku plačilne kartice 4 – Šifriranje prenosa podatkov o imetniku plačilne kartice preko odprtih, javnih omrežjih
Vzdrževati program za upravljanje z ranljivostmi sistema	5 – Uporabljati in redno posodabljati protivirusno programsko opremo ali programe 6 – Razvijati in vzdrževati varne sisteme in aplikacije
Implementacija ukrepov za kontrolo dostopa do občutljivih kartičnih podatkov	7 – Omejitev dostopa do podatkov o imetniku plačilne kartice na najmanjši obseg, ki je potreben za izvršitev transakcije 8 – Dodeliti edinstveno identifikacijsko številko vsaki osebi, ki ima dostop do informacijske podpore 9 - Omejiti fizični dostop do podatkov o imetniku plačilne kartice
Redno spremljanje in testiranje omrežij	10 – Slediti in nadzorovati vse dostope do omrežnih virov in do podatkov o imetniku plačilne kartice 11 – Redno testiranje varnostnih sistemov in procesov
Vzdrževanje politike varovanja informacij	12 – Vzdrževati politiko, ki ureja področje varnosti informacij in velja za zaposlene in pogodbene izvajalce

Zahteve PCI DSS

Poleg naštetih kontrol še:

- natančna opredelitev področja, kjer je zahteve potrebno upoštevati;
- način opredelitve obsega izvajanja varovanja informacij po PCI DSS;
- način dokazovanja skladnosti z zahtevami PCI DSS.

FMC
FMC Group



Lou thought he was lost, but then he saw the sign.

FMC Group

FMC
FMC Group

Kako uvajati skladnost s PCI DSS

Opredelitev obsega varovanja po PCI DSS s pomočjo:

- z avtomatskim iskalnikom se po bazah podatkov, datotečnih sistemih ipd. se poiščejo tisti viri, ki vsebujejo podatke o plačilnih karticah in njihovih imetnikih;
- podatke v fizični obliki je potrebno poiskati z analizo poslovnih procesov.

FMC
FMC Group

Kako uvajati skladnost s PCI DSS

nad.

Kartični poslovni procesi:

- otvoritev/sprememba kartičnega računa/kartice,
- izdelava kartice,
- izplačilo gotovine (bančno okence, ATM),
- avtorizacija,
- knjiženje nakupov,
- poravnava med članicami (vključno s poročili),
- plačilo trgovcem (vključno z izpiskom),
- plačilo imetnika (vključno z izpiskom),
- finančne reklamacije,
- spremljava,
- knjigovodstvo,
- analize,
- poročanje,
- arhiv,
- razvoj in testiranje

FMC
FMC Group

Kako uvajati skladnost s PCI DSS

nad.

V vsakem procesu je treba ugotoviti:

- ka
- ka
- ka iporabljeni.

V na

- ali eni,
- ali ni,
- na kakšen način se bodo ugotovljeni podatki varovali.

FMC Group

FMC
FMC Group

Učinkovitost PCI DSS

Tip zlorabe	Način kraje podatkov	PCI DSS zahteva
Skimming	Skimming na POS terminalih	2 – Ne uporabljati privzetih nastavitev, ki jih dobavi prodajalec sistema, za sistemska gesla in druge varnostne parametre 8 – Dodeliti edinstveno identifikacijsko številko vsaki osebi, ki ima dostop do informacijske podpore 9 – Omejiti fizični dostop do podatkov o imetniku plačilne kartice 10 – Slediti in nadzorovati vse dostope do omrežnih virov in do podatkov o imetniku plačilne kartice 12 – Vzdrževati politiko, ki ureja področje varnosti informacij in velja za zaposlene in pogodbene izvajalce
	Skimming na bančnih avtomatih	Ni primerno, drugi načini zmanjševanja tveganj (antiskimming naprave)
	Drugi načini skimminga	2 – Ne uporabljati privzetih nastavitev, ki jih dobavi prodajalec sistema, za sistemska gesla in druge varnostne parametre 8 – Dodeliti edinstveno identifikacijsko številko vsaki osebi, ki ima dostop do informacijske podpore 9 – Omejiti fizični dostop do podatkov o imetniku plačilne kartice 10 – Slediti in nadzorovati vse dostope do omrežnih virov in do podatkov o imetniku plačilne kartice 12 – Vzdrževati politiko, ki ureja področje varnosti informacij in velja za zaposlene in pogodbene izvajalce

Učinkovitost PCI DSS

Tip zlorabe	Način kraje podatkov	PCI DSS zahteva
Kartica ni prisotna	Vdor v sistem trgovca, procesnega centra, banke ipd.	Vse zahteve PCI DSS
Kraja identitete (identity theft)	Kraja podatkov pri imetniku plačilne kartice	Ni primerno, drugi načini zmanjševanja tveganj (ozaveščanje imetnikov kartic)
Vdor v bančni avtomat	Vdor v sistem posameznega bančnega avtomata	Vse zahteve PCI DSS
BIN attack	Ni kraje podatkov	Ni primerno, drugi načini zmanjševanja tveganj (kvalitetna avtorizacija)

Za zaključek

Prihodnost:

- izvajanje plačilnih storitev na novih tehnologijah
- vedno novi in inovativni načini za izvedbo zlorabe
- zaostritev varnostnih zahtev za vse udeležence v procesu uporabe plačilnih kartic in vpeljava novih zahtev na področju preprečevanja odtekanja informacij preko pooblaščenih uporabnikov
- PCI DSS ima velike ambicije, da postane splošno veljavni standard na področju finančne industrije

FMC
FMC Group

Vaša vprašanja?

Veliko uspehov pri poslovanju s plačilnimi karticami!

alenka.glas@fmc.si

FMC
FMC Group