First Data.

Ievads Maksājumu karšu nozares Datu drošības standartā

Mācību materiāls uzņēmumu vadītājiem un banku speciālistiem

Valters Paiders
Kvalitātes un atbilstības vadītājs *First Data* uzņēmumos Baltijas valstīs

Lūdzu, atbildiet uz šādiem jautājumiem!

- Uzņēmuma datorsistēmās glabājas maksājumu karšu numuri (jā/nē)
- Uzņēmuma klienti veic vairāk nekā 1 milj. maksājumu karšu transakciju gadā (jā/nē)
- Klienti veic pirkumu samaksu internetā vai nosaucot maksājumu karšu datus pa tālruni (jā/nē)
- Uzņēmumā glabājas POS terminālu kvītis vai citi dokumenti, uz kuriem pilnībā vai daļēji redzams kartes numurs (jā/nē)
- Uzņēmumā reiz tika nozagtas iekārtas vai dokumenti, kas saturēja maksājumu karšu numurus (jā/nē)
- Uzņēmums veic maksājumu karšu darījumu informācijas pārsūtīšanu (jā/nē)
- Uzņēmums izmanto pašu pirktas iekārtas un sistēmas maksājumu karšu pieņemšanai (jā/nē)

First Data.

Maksājumu karšu nozares standarti

- Ja atbildējāt “jā” vismaz uz vienu jautājumu, uzņēmumam ir aktuāla prezentācijā ietvertā informācija, jo tam jānodrošina atbilstība Maksājumu karšu nozares standartiem.

KĀPĒC?

- Nodrošinot atbilstību šiem standartiem, līdz minimumam samazināsiet uzņēmuma riskus, ko rada karšu datu zādzības. Arī zināšanās jūs ieguldāt šodien, lai gūtu pārliecību un priekšrocības rīt.

First Data.

Maksājumu karšu nozares standarti

- Kas ir Maksājumu karšu nozares Datu drošības standarts (Payment Card Industry Data Security Standard – PCI DSS)?

  Maksājumu karšu nozares Datu drošības standarts ir minimālās drošības prasības, kuras jāievēro katram, kas veic karšu darījumu apstrādi, glabāšanu un pārraidi.

- Kas ir Maksājumu karšu nozares PIN drošības standarts (Payment Card Industry PIN Security Standard – PCI PIN)?

  Maksājumu karšu nozares PIN drošības standarts ir minimālās drošības prasības, kuras jāievēro katram, kas veic PIN kodu apstrādi un pārraidi.

- Kas ir Maksājumu aplikāciju Datu drošības standarts (Payment Application Data Security Standard – PA DSS)?

  Maksājumu aplikāciju Datu drošības standarts ir minimālās drošības prasības programmatūrai, kas veic karšu darījumu apstrādi.

First Data.

Maksājumu karšu nozares standarti

Kāpēc ieviesti šie standarti?

- Tehnoloģiju attīstība sniegusi daudzas ērtības – mūsdienās varam skatīties televīziju, lasīt laikrakstus un jaunākās ziņas, samaksāt rēķinus, neizejot no mājas.
- Diemžēl tehnoloģiskos sasniegumus izmanto arī negodīgi cilvēki, lai neatļauti piekļūtu uzņēmumu sistēmām ar mērķi iegūt konfidenciālu informāciju, kuru vēlāk varētu izmantot, gūstot sev labumu.
- Tur, kur ir nauda, vienmēr atradīsies kāds, kas grib to nozagt. Ja nesargāsi sevi, arī Dieviņš tevi nesargās. Šīs divas parunas tieši var attiecināt uz maksājumu karšu informāciju. Maksājumu karšu dati, ja tie nokļuvuši negodīgu cilvēku rokās, ļoti īsā laikā var radīt milzīgus zaudējumus un nepatikšanas.

First Data.

Maksājumu karšu nozares standarti

- Maksājumu karšu pieņēmējam jānodrošina atbilstība visiem minētajiem standartiem.
- Prezentācijā sīkāk tiks analizēts Maksājumu karšu nozares Datu drošības standarts.
  - Prezentācijas beigās – daži ieteikumi attiecībā uz PIN koda ievades iekārtām (aktuāli tikai tiem tirgotājiem, kuri paši iegādājas un uzstāda šīs iekārtas).
  - Maksājumu aplikāciju Datu drošības standarts attiecas tikai uz programmatūras piegādātājiem. Tas nozīmē, ka, pirms iegādājas programmatūru, kas apstrādā maksājumu karšu datus, izdevējam jāpieprasa pierādījumi, ka programmatūra atbilst šim standartam (šādas programmatūras, t.sk. instalētās, atbilstība ir obligāta ar 2012. gada 1. jūliju).

First Data.

Copyright 2008, First Data Corporation. All Rights Reserved.

Saturs

1. Maksājumu karšu nozares Datu drošības standarts
   - Vēsture.
   - Standarta piemērošanas jomas. Piemēri.
   - Saskaņošana ar citiem standartiem un tiesību aktiem.
   - Standarta trīs pīlāri.
2. Maksājumu karšu īpatnības
   - Maksājumu karšu uzbūve. Aizliegtie dati.
   - Informācijas nesēji uz norēķinu kartes, to saturs.
3. Standarta neievērošanas sekas
   - Soda naudas un citi sarežģījumi.
   - Karšu datu zādzība – vai vienmēr tiks piemērots sods?
   - Ja noticis starpgadījums…
4. Mācāmies no citu kļūdām
5. Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei

First Data.

1. Maksājumu karšu nozares Datu drošības standarts. Vēsture I

Maksājumu karšu nozares Datu drošības standarts ir viens no jaunākajiem standartiem pasaulē.

- Pirmsākums – 2000. gadā maksājumu karšu organizācijas, izvērtējot tehnoloģiju attīstību un ar to saistītos riskus, izveidoja specifiskus noteikumus karšu datu aizsardzībai:
  - » *VISA CISP (Cardholder Information Security Program)*;
  - » *MasterCard SDP (Site Data Protection)* programma;
  - » *DISC (Discovery Information Security Compliance)*;
  - » *American Express DSS (Data Security Standard).*
- 2004. gadā šie noteikumi tika apvienoti un standartizēti, izveidojot vienotu standartu – Maksājumu karšu nozares Datu drošības standartu (*Payment Card Industry Data Security Standard;* PCI DSS).
- 2006. gadā starptautiskās karšu organizācijas, auditorkompānijas, bankas un karšu apstrādes centri izveidoja Datu drošības standarta padomi *(PCI Security Standards Council),* kuras pārziņā pilnībā tika nodots standarts.
- 2007. gadā Datu drošības standarta padome pilnībā pārņēma PIN ievades iekārtas un ar tām saistīto drošības jautājumu izskatīšanu un lēmumu pieņemšanu.

First Data.

1. Maksājumu karšu nozares Datu drošības standarts. Vēsture II

Neraugoties uz drošības prasību konsolidāciju, starptautiskās karšu organizācijas joprojām uztur īpašus noteikumus saistībā ar karšu drošības prasībām:

- *VISA AIS (Account Information Security)* programmu;
- *MasterCard SDP (Site Data Protection)* programmu;
- *American Express DSS (Data Security Standard)* programmu.

Šīs programmas nosaka specifiskas prasības attiecībā uz karšu pieņēmējiem – tirgotājiem un maksājumu apstrādes centriem.

First Data.

1. Maksājumu karšu nozares Datu drošības standarts: VISA, *MasterCard*

Līmenis	Tirgotājs	Prasība
1.	Vairāk nekā 6 milj. karšu darījumu gadā vai notikusi karšu datu zādzība pie tirgotāja	Reizi gadā – audits, ko veic sertificēta auditorkompānija, vai aizpildīta pašnovērtējuma anketa, ko veic sertificēts iekšējais auditors. Reizi ceturksnī – uzņēmuma datortīkla ārējā pārbaude.
2.	1–6 milj. karšu darījumu gadā	Reizi gadā – aizpildīta pašnovērtējuma anketa, ko veic sertificēts iekšējais auditors, vai audits, ko veic sertificēta auditorkompānija. Reizi ceturksnī – uzņēmuma datortīkla ārējā pārbaude.
3.	20 tūkst.–1 milj. e-komercijas darījumu gadā	Reizi gadā – jāaizpilda pašnovērtējuma anketa *(self-assessment questionnaire)*. Reizi ceturksnī – uzņēmuma datortīkla ārējā pārbaude.
4.	Visi pārējie tirgotāji	Veicamās darbības nosaka pieņēmējbanka.

Sīkāka informācija https://www.pcisecuritystandards.org/saq/instructions_dss.shtml.

First Data.

1. Maksājumu karšu nozares Datu drošības standarts: VISA, *MasterCard*

Tirgotāju dalījums (VISA un *MasterCard)*.

Karšu darījumu skaits tiek aprēķināts reizi ceturksnī. Tiek ņemti vērā visi karšu darījumi (veiksmīgie, atteiktie, kredītdarījumi utt.).

Karšu darījumu skaits tiek aprēķināts katrai karšu shēmai atsevišķi:

- VISA + *VISA Electron* + *V PAY*;
- *MasterCard* + *MasterCard Electronic* + *Maestro*.

First Data.

1. Maksājumu karšu nozares Datu drošības standarts: *American Express*

Līmenis	Tirgotājs	Prasība
1.	Vairāk nekā 2.5 milj. karšu darījumu gadā vai notikusi karšu datu zādzība no tirgotāja	Reizi gadā – audits, ko veic sertificēta auditorkompānija. Reizi ceturksnī – uzņēmuma datortīkla ārējā pārbaude.
2.	50 tūkst.–2.5 milj. karšu darījumu gadā	Reizi ceturksnī – uzņēmuma datortīkla ārējā pārbaude.
3.	Mazāk par 50 tūkst. karšu darījumiem gadā	Veicamās darbības nosaka pieņēmējbanka.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Trīs pīlāri

Aizsardzība – viss, kas nav atļauts, ir aizliegts

- Drošības sistēmu (ugunsmūra, ielaušanās brīdināšanas sistēmas u.c.) izmantošana un uzturēšana.
- Lietotāju kontu paroļu izmantošana, datu šifrēšana, pierakstu veidošana.
- Fiziskās pieejas ierobežošana un kontrole (videonovērošana, pieejas kontroles sistēmas).

Audits un kontrole

- Nepārtraukta sistēmu uzraudzība un izņēmumu protokolēšana.
- Regulāra drošības sistēmu un procesu pārbaude.
- Regulāra sistēmu konfigurācijas un pierakstu pārbaude (drošības auditi).
- Jebkuru pārmaiņu apstiprināšana pirms to ieviešanas.
- Nevajadzīgās informācijas droša iznīcināšana.

Mācības un informēšana visos līmeņos

- Jaunākie informācijas tehnoloģiju drošības draudi.
- Informācijas drošības politikas ieviešana un izplatīšana.
- Informētība par drošību.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Joma I

Maksājumu karšu nozares Datu drošības standarts attiecas uz visu, kas tieši vai netieši nonāk saskarē ar karšu datiem.

Joma, ko aptver standarts:

- karšu datu apstrāde;
- karšu datu pārraide;
- karšu datu glabāšana.

Standarts tieši nosaka prasības:

- uzņēmuma datortīklu infrastruktūrai;
- programmatūrai.

Standarts pastarpināti nosaka:

- dokumentu, kas satur karšu datus, glabāšanas un aizsardzības prasības;
- prasību, ka karšu datu apstrādē un pārraidē iesaistītajiem pakalpojumu sniedzējiem jāpierāda atbilstība šim standartam.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Joma II

Ja uzņēmums vai kāda tam piederoša sistēma **neglabā, neapstrādā** un **nepārraida** karšu datus, Maksājumu karšu nozares Datu drošības standarts **neattiecas** uz šo uzņēmumu (sistēmu).

Tātad, **ja** uzņēmumā **nav veikta** datortīkla **sadalīšana**, **atsevišķi nodalot** to daļu, kurā notiek **karšu datu** apstrāde, Maksājumu karšu nozares Datu drošības standarta **prasības attiecas uz pilnīgi visu** uzņēmuma informācijas infrastruktūru.

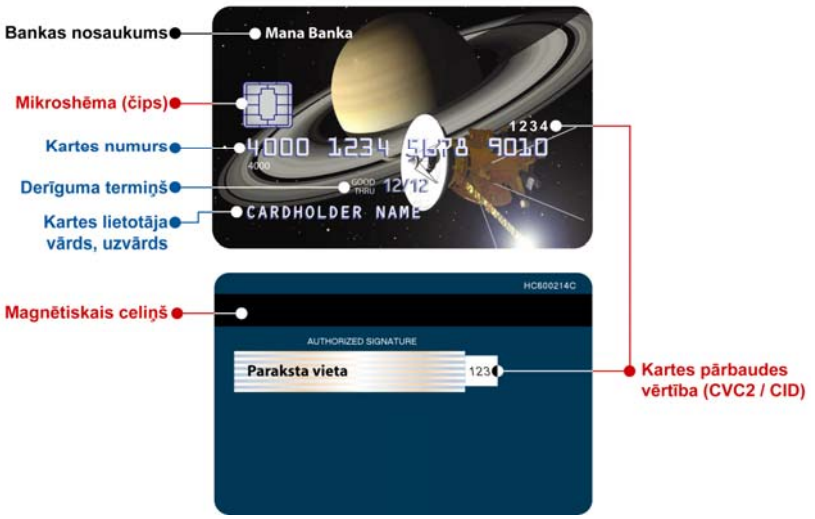
First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Joma III

	Elements	Drīkst uzglabāt?	Ir jāaizsargā?	Standarts 3.4
Drīkst uzglabāt: * ja glabā kopā ar kartes numuru, ir jānodrošina aizsardzība	Kartes numurs	+	+	+
	Kartes lietotājs*	+	+*	–
	Servisa kods*	+	+*	–
	Derīguma termiņš*	+	+*	–
UZGLABĀT NEDRĪKST!	Pilna celiņa dati	–	X	X
	CVC2/CVV2/CID	–	X	X
	PIN / PIN Block	–	X	X

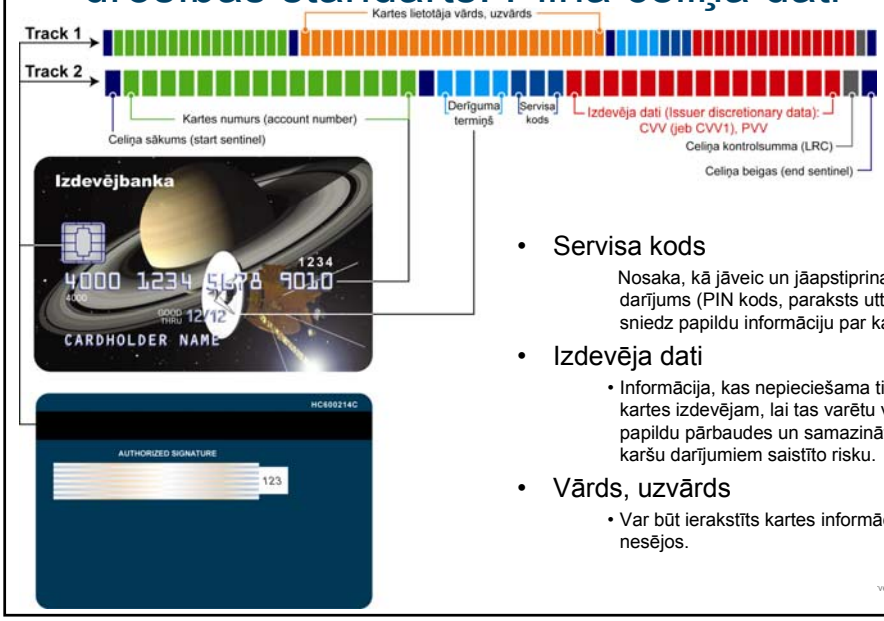
First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Kartes uzbūve



First Data.

2. Maksājumu karšu nozares Datu drošības standarts. Pilna celiņa dati



- Servisa kods

  Nosaka, kā jāveic un jāapstiprina darījums (PIN kods, paraksts utt.), un sniedz papildu informāciju par karti.

- Izdevēja dati
  - Informācija, kas nepieciešama tikai kartes izdevējam, lai tas varētu veikt papildu pārbaudes un samazināt ar karšu darījumiem saistīto risku.
- Vārds, uzvārds
  - Var būt ierakstīts kartes informācijas nesējos.

ved.

2. Maksājumu karšu nozares Datu drošības standarts. Pilna celiņa dati

Izdevēja dati nepieciešami tikai kartes izdevējam un tikai darījuma autorizācijas procesā. Pēc tam tie nav vajadzīgi.

Šo datu glabāšana dod iespēju viegli izgatavot kartes dublikātu un to izmantot krāpniecisku darījumu veikšanai.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts: prioritātes

Maksājumu karšu nozares Datu drošības standartu padome izstrādājusi karšu datu aizsardzības ieviešanas prioritātes, kas numurētas no 1 līdz 6.

Starptautiskās karšu organizācijas rekomendē tirgotājiem veikt Datu drošības standarta ieviešanu, vadoties pēc prioritātēm.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts: pašnovērtējums

- Aktuālā versija atrodas PCI interneta resursā (www.pcisecuritystandards.org).
- Pašnovērtējuma apjoms ir atkarīgs no tirgotāja specifikas:
  - e-komercijas tirgotājiem, kuri izmanto *First Data* piegādāto IBIS risinājumu un paši neapstrādā karšu datus, jāaizpilda A variants;
  - tirgotājiem, kuri kartes pieņem ar imprintera un/vai atsevišķa POS termināļa palīdzību un karšu datus neglabā elektroniski, jāaizpilda B variants;
  - tirgotājiem, kuri kartes pieņem POS sistēmās/kasu sistēmās, kas karšu datus sūta, izmantojot internetu, bet karšu datus neglabā elektroniski, jāaizpilda C variants;
  - tirgotājiem, kuri neietilpst nevienā no minētajām kategorijām, jāaizpilda D variants.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts: pašnovērtējums

- Lai veiktu pašnovērtējumu, tirgotājam jāidentificē visi kanāli, pa kuriem uzņēmumā ienāk vai iziet karšu dati, kā arī vietas, kur karšu dati tiek glabāti. Piemēram:
  - POS termināļa drukātās kvītis ar kartes numuru (arī, ja numurs ir maskēts);
  - bankas sūtītie dokumentu pieprasījumi, karšu reklamāciju dokumenti;
  - rezervācijas pieteikumi pa e-pastu (ja satur karšu datus);
  - viesu reģistrācijas sistēma viesnīcās (ja satur karšu datus);
  - skapis grāmatvedībā, kurā glabājas kases žurnāls kopā ar termināļu kvītīm, u.tml.
- Veicot pašnovērtējumu, jāizvērtē visu identificēto kanālu un karšu datu glabāšanas vietu atbilstība standarta prasībām.

First Data.

Copyright 2008, First Data Corporation. All Rights Reserved.

2. Čipu tehnoloģijas ietekme uz tirgotāja atbilstību

Tirgotājiem, kas veic VISA/*MasterCard* zīmola čipkaršu pieņemšanu, pēc bankas ieskatiem var tikt piemērotas atvieglotas prasības, ja:

- tirgotājs gadā apstrādā vismaz 1 milj. darījumu un
- vismaz 95% no visiem darījumiem veikti, izmantojot čipu tehnoloģiju, un
- čipkaršu pieņemšanas iekārtām ir derīgi *EMVCo Type I* un *Type II* sertifikāti, un
- tirgotājs neglabā sensitīvus karšu autentifikācijas datus, un
- tirgotājs ir pilnībā nodalījis e-komercijas infrastruktūru, un
- pie tirgotāja pēdējo 12 mēnešu laikā nav notikuši karšu datu zādzības gadījumi, un
- tirgotājs reizi gadā kopā ar pieņēmējbanku veic karšu datu zādzības incidentu pārvaldības procedūru pārbaudi saskaņā ar dokumentā *What to do if compromised ietvertajām* VISA vadlīnijām.

Šādiem tirgotājiem jānodrošina atbilstība PCI DSS standarta daļai, kas noteikta ar 1.–4. prioritāti (nevis visam standartam).

Atviegloto prasību piemērošana neatbrīvo tirgotāju no pienākuma nodrošināt atbilstību Datu drošības standartam!

First Data.

2. Maksājumu karšu nozares Datu drošības standarts un citi standarti I

- Kvalitātes vadības sistēma (ISO 9001:2008)

  Iekšējie auditi, korektīvās darbības – procedūras iespējams paplašināt, iekļaujot tajās drošības auditus un auditu rezultātu ziņošanas kārtību, kā arī auditos atklāto nepilnību novēršanu.

  Nepieciešamās zināšanas un kompetence (6.2.), informēšana par pārmaiņām (7.2.) – esošajos procesos nepieciešamas nebūtiskas pārmaiņas, lai tos pielāgotu arī šim standartam.

  Produkta īstenošana (7. nodaļa) – raugoties no Datu drošības standarta viedokļa, ir nepieciešama.

- ISO 9001:2008 standarta prasība (7.5.4.) par klientu īpašuma aizsardzību nosaka Datu drošības standarta ieviešanas nepieciešamību uzņēmumā, kas apstrādā karšu datus.

First Data.

2. Maksājumu karšu nozares Datu drošības standarts un citi standarti II

- Personas datu aizsardzības likums

  Nosaka personas datu apstrādi, kā arī identificē nepieciešamību aizsargāt personas datus. Papildus tam normatīvie akti nosaka tehniskās prasības šo datu aizsardzībai, kas ir līdzīgas Maksājumu karšu nozares Datu drošības standarta prasībām. Karšu dati pieskaitāmi personas datiem.

- Informācijas drošības standarts ISO 27002:2005

  Datu drošības standarts pēc būtības ir šā standarta pamats, uzņēmumam, kas jau atbilst minētā standarta prasībām, jāveic minimālas pārmaiņas esošajās procedūrās un procesos, precizējot aspektus, kas attiecas tieši uz karšu datiem un to aizsardzību.

- SEPA apņemšanās
  - Līdz ar eiro ieviešanu SEPA apņemšanās oficiāli stāsies spēkā.

First Data.

3. Maksājumu karšu dati un krāpniecības tendences

Gads	Krāpnieka portrets	Krāpnieka mērķis	Galvenie krāpniecības veidi	Krāpnieku iecienītie karšu veidi	Krāpniecības veikšanai nepieciešams
1980.	• Atsevišķi indivīdi	• Karšu lietotāji	• Darījumi ar zagtām, pazaudētām un pārtvertām kartēm	• *Travel & Entertainmnent* kredītkartes (piemēram, *American Express*)	• Iespēja
1990.	• Nelielas grupas	• Atsevišķi mazumtirgotāji	• Lokālo karšu viltošana un neatļauta karšu datu nolasīšana	• *Gold*, *Platinum* u.tml. kredītkartes	• Minimālas zināšanas
2000.	• Lokālas organizētās noziedzības bandas	• Mazumtirgotāji	• Datu zādzības no sistēmām, pikšķerēšana *(phishing)*	• Jebkuras kredītkartes	• Tehniskas zināšanas par izmantotajām sistēmām
Pašlaik	• Starptautiskas organizētās noziedzības bandas	• Bankas • Karšu apstrādes centri, lielie mazumtirgotāji	• Globālas datu zādzības, zagto karšu datu izmantošana pirkumiem internetā un naudas izņemšanai bankomātos	• Jebkuras kartes	• Bezkaunība, drosme • Ļoti detalizētas tehniskas zināšanas • Iekšējā informācija • Globāli sakari

First Data.

3. Standarta neievērošanas sekas

Maksājumu karšu nozares Datu drošības **standarta neievērošana** uzņēmumam sagādās **milzīgas nepatikšanas un zaudējumus**.

First Data.

3. Standarta neievērošanas sekas I

Soda naudas

- VISA – soda nauda 10 tūkst.– 50 tūkst. eiro (atkarīga no tirgotāja darbības apjoma)
  + 30 tūkst. eiro mēnesī, ja glabāti aizliegtie dati.
- *MasterCard* – līdz 100 tūkst. ASV dolāru par katru standarta punkta pārkāpumu + soda nauda 500–250 000 eiro (atkarīga no zādzības apmēra).
- *American Express* – līdz 100 tūkst. ASV dolāru.

Finansiāla atbildība

Visi krāpnieciskie darījumi ar kartēm, kuras bijušas pie šā tirgotāja, jāapmaksā tirgotājam, pat ja darījums noticis pie cita tirgotāja.

- VISA – maksimālā atbildība 1 milj. ASV dolāru.
- *American Express* – maksimālā atbildība 3 milj. ASV dolāru.
- *MasterCard* – maksimālā atbildība netiek ierobežota. Papildus jāmaksā kompensācija izdevējbankām par karšu atkārtotu izdošanu un klientu apkalpošanu 3% apmērā un papildu kompensācija 5% apmērā, ja bijuši krāpnieciskie darījumi.

Ja tirgotājs glabājis arī PIN, maksimālā atbildība netiek ierobežota.

First Data.

3. Standarta neievērošanas sekas II

Tiesvedība

Juridiskās sekas – kriminālietas par pieļautajiem likumpārkāpumiem, civilprasības par zaudējumu segšanu.

Negatīva publicitāte

Uzņēmums zaudē lojālos klientus.

First Data.

3. Standarta neievērošanas sekas. Karšu datu zādzība

Kādos gadījumos tiks aprēķinātas soda naudas un noteikta finansiāla atbildība par krāpniecības radītajiem zaudējumiem?

Tikai tajos gadījumos, kad kartes pieņēmējs nav ievērojis Maksājumu karšu nozares Datu drošības standarta prasības.

Kā noteikt, vai standarts ir pārkāpts vai ne?

Ja notikusi neatļauta piekļuve datorsistēmām, to inficēšana ar jebkādiem datorvīrusiem, fiziskas iekārtas (datora, servera) vai datu nesēja (rezerves kopijas lentes, kompaktdiska, cietā diska u.c.) vai dokumentu ar karšu datiem (piemēram, POS terminālu kvīšu ar pilnu kartes numuru) zādzība, tas uzskatāms par standarta pārkāpumu.

First Data.

3. Standarta neievērošanas sekas. Starpgadījumi I

Konstatējot karšu datu zādzību, uzņēmums:

- nekavējoties par to ziņo pieņēmējbankai;
- nekavējoties par to ziņo policijai;
- norīko atbildīgo, kas turpmāk koordinēs izmeklēšanu;
- ja notikusi ielaušanās uzņēmuma datorsistēmās, uzlauztās datorsistēmas izolē un saglabā tādā stāvoklī, kādas tās bija brīdī, kad konstatēts ielaušanās fakts (uzlauztās datorsistēmas nekādā gadījumā nedrīkst pārstartēt, izslēgt, mēģināt lietot tastatūru).

Ko dara pieņēmējbanka?

- Pieņēmējbanka par notikušo paziņo starptautiskajām karšu organizācijām un kopā ar tirgotāju noslēdz līgumu ar sertificētu drošības auditoru, kas ieradīsies uzņēmumā, lai veiktu sīku izmeklēšanu un novērtētu uzņēmuma atbilstību Maksājumu karšu nozares Datu drošības standartam.

First Data.

3. Standarta neievērošanas sekas. Starpgadījumi II

Ko darīs auditori

- Auditori veiks ļoti detalizētu uzņēmuma un tā pārziņā esošo datorsistēmu izpēti un to atbilstības novērtēšanu, par visām atklātajām neatbilstībām informējot uzņēmuma vadību.
- Uzņēmuma vadībai nekavējoties jānovērš atklātās neatbilstības vai jāizveido neatbilstību novēršanas laika plāns, vai jāveic darbības, kas kompensē neatbilstības radītos trūkumus.

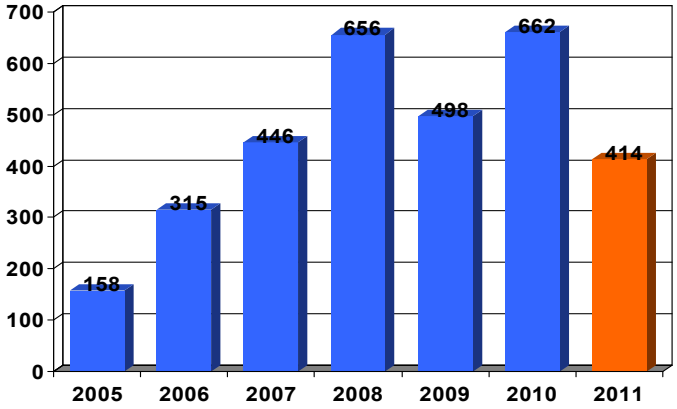
Sekas

- Uzņēmums bankai atmaksā soda naudas, kuras tai aprēķinājušas starptautiskās karšu organizācijas.
- Uzņēmums noslēdz līgumu ar sertificētu auditorkompāniju, kas uzņēmumā katru gadu veiks Maksājumu karšu nozares Datu drošības standarta auditu, kā arī reizi ceturksnī veiks uzņēmuma datortīklu ārējo pārbaudi.

First Data.

3. Standarta neievērošanas sekas. Statistika

Reģistrēto IT drošības incidentu un datu zādzību skaita dinamika



Avots: http://www.idtheftcenter.org/.

First Data.

4. Mācāmies no citu kļūdām. *TJX Companies* I

2006. gada decembrī hakeri ielauzās ASV lieltirgotavas *TJX Companies* datorsistēmās.

Sākotnējās oficiālās aplēses

Nozagti 45.7 milj. karšu datu.

455 tūkst. klientu nozagti personas dati.

– Pirmie izmeklēšanas rezultāti

Uzņēmuma datorsistēmās glabājās kartes magnētiskā celiņa kopijas (vēlāk izmeklētāji oficiāli paziņoja, ka kopā ar karšu datiem nozagti arī PIN kodi).

– Finansiālie zaudējumi

1 mēneša laikā – 3.5 milj. ASV dolāru.

– Negatīva publicitāte

Ļoti daudzi klienti, uzzinot, ka tirgotājs nav rūpējies par karšu datu drošību, pārtrauc sadarbību ar uzņēmumu.

First Data.

4. Mācāmies no citu kļūdām. *TJX Companies* II

2007. gada februāris

- Uzņēmuma zaudējumi sasnieguši 7.5 milj. ASV dolāru.

2007. gada marts

- Ar karšu datiem, kas nozagti *TJX Companies*, ASV īstenota vērienīga krāpniecības shēma 8 milj. ASV dolāru apmērā.

2007. gada maijs

- Ziņu aģentūru žurnālisti uzzināja, ka no uzņēmuma nozagti aptuveni 200 milj. karšu datu. Uzņēmums šo informāciju nosauc par žurnālistu izdomājumiem, piebilstot, ka patiesos apmērus uzzināt neizdosies. Eksperti lēš, ka uzņēmumam nāksies investēt 1 mljrd. ASV dolāru, lai sakārtotu infrastruktūru.

2007. gada decembris

- *TJX Companies* paziņo, ka karšu datu zādzības dēļ uzņēmumam radīti zaudējumi 197 milj. ASV dolāru apmērā. Uzlaušanas seku likvidēšanai uzņēmums rezervēja 338 milj. ASV dolāru.
- Pret uzņēmumu ierosinātas ļoti daudzas tiesas prāvas.

First Data.

4. Mācāmies no citu kļūdām. *TJX Companies* III

Kāpēc bija iespējama šāda datu zādzība?

- Uzņēmumā lietoja cenu marķierus, kas izmantoja bezvadu tehnoloģiju *(WiFi)*. Šie marķieri sazinājās ar kasēm, un tās "informēja" par preci un tās cenu.
- Hakeri, izmantojot marķieru nepilnības (marķieros netika izmantotas drošas bezvadu tehnoloģijas) un īpašu antenu, radīja savu "cenu marķieri", ar kuru iekļuva kases sistēmās.
- Kases sistēma nebija aprīkota ar antivīrusu programmu, un tajā nebija instalēti operētājsistēmas ražotāja drošības ielāpi. Izmantojot drošības caurumus, hakeri izveidoja savus lietotāja kontus un ielauzās lielveikala serveros, kas apstrādāja darījumus. Ielaušanos būtiski atviegloja tas, ka uzņēmumā netika izmantoti ugunsmūri *(firewalls)*.
- Karšu dati, kas glabājās šajos serveros, nebija šifrēti. Hakeri tos savāca, šifrēja un šifrētos failus pārkopēja savos datoros. Uzlauzēju grupa darbojās ļoti saskaņoti – lielveikala sistēmā viņi bija atstājuši ziņojumus, lai "kolēģi" nedarītu dubultu darbu.
- Izmeklēšanas gaitā šifrētie faili tika atrasti, taču tos atšifrēt neizdevās.

First Data.

4. Mācāmies no citu kļūdām. Statistika

Pieci svarīgākie iemesli, kāpēc notiek datu zādzības:

1. uzņēmums neveic ražotāja vai noklusēto *(default)* lietotāja kontu un paroļu nomaiņu;
2. datu bāzes vaicājumu neatļauta modificēšana *(SQL Injections)*;
   - izmantojot datubāzes/aplikācijas nepilnības, uzbrucējs veic vaicājuma modificēšanu ar mērķi iegūt nepublicējamus datus no datu bāzes.
3. nepietiekama datortīkla aizsardzība;
4. uzņēmums neveic drošības pārbaudi (sistēmu skenēšanu);
5. uzņēmums neveic drošības sistēmu uzraudzību reālajā laikā;
6. uzņēmums savlaicīgi neveic programmatūras ražotāja drošības atjauninājumu instalēšanu.

Avots: MasterCard, VISA Europe

First Data.

4. Mācāmies no citu kļūdām. Neefektīva drošības ielāpu vadība

Saskaņā *ar Secunia.com* informāciju* Latvijā vienā personālajā datorā ir vidēji 3 – 4 datorprogrammas, kas satur drošības riskus.

– Tā kā *Secunia* analizē programmproduktus, kas ir ļoti plaši izplatīti, personālo datorsistēmu inficēšanās risks vērtējams kā ļoti liels (labākās antivīrusu programmas spēj atpazīt tikai 98% no visiem zināmajiem vīrusiem).

First Data.

4. Mācāmies no citu kļūdām. Statistika

Datu zādzības visbiežāk notiek:

- pie interneta pakalpojumu sniedzējiem;
- pie maksājumu sistēmu koncentratoriem *(payment system gateways)*;
- pie maksājumu apstrādes pakalpojumu sniedzējiem *(third party processors)*;
- bezvadu tīklā *(WiFi Networks)*;
- kaitnieciskas programmatūras (datortīkla informācijas okšķeri *(packet sniffers)*) instalēšanas rezultātā;
- nedrošas POS programmatūras dēļ;
- aparatūras un iekārtu zādzību dēļ.

Avots: MasterCard.

First Data.

4. Mācāmies no citu kļūdām. Atbildība I

Par karšu datu nozagšanu un nelikumīgu izmantošanu tiek piemērots Latvijas Republikas Krimināllikuma 193. pants, kas paredz brīvības atņemšanu līdz 15 gadiem ar mantas konfiskāciju,

BET,

ja būsiet iesaistīts apjomīgā karšu datu zādzībā un jūs notvers **citā valstī**, pastāv varbūtība, ka jūs notiesās pēc **šīs valsts likumiem.**

First Data.

4. Mācāmies no citu kļūdām. Atbildība II

- Pēc *TJX Companies* datortīkla uzlaušanas sākās apjomīga izmeklēšana daudzās pasaules valstīs.
- Viens no šīs zādzības organizatoriem – Ukrainas pilsonis Maksims Jastrevskis *(Maksik)* – tika aizturēts Turcijā.

  Tā kā *TJX* uzlaušanas gadījumā Turcijas bankas bija cietušas ~35 tūkst. ASV dolāru lielus zaudējumus, Turcijas varas iestādes nolēma neizdot aizturēto Ukrainas pilsoni ASV, bet notiesāja viņu Turcijā, piespriežot 30 gadu ieslodzījumā.

First Data.

5. Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei I

- Viedkaršu pieņemšanas iekārtām to iegādes brīdī jābūt derīgiem šādiem EMVCo sertifikātiem:
  - *EMVCo Type 1 Approval*;
  - *EMVCo Type 2 Approval*.
- Stingri iesakām pirms iegādes pārliecināties par izvēlētās iekārtas atbilstību, pieprasot attiecīgo informāciju no piegādātāja un pārbaudot to interneta resursā www.emvco.com.

First Data.

5. Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei II

Iekārtām, kuras tiks izmantotas PIN koda ievadei, obligāti jābūt sertificētām.

- Uzņēmumam stingri iesakām pirms šo iekārtu iegādes pieprasīt iekārtu piegādātājam informāciju par PIN ievades iekārtas modeli, sērijas numuru *(hardware number)* un programmatūras versiju *(firmware number)*.

Modelim un sērijas numuram, un programmatūras versijai jāsakrīt ar interneta resursā www.pcisecuritystandards.org publicēto informāciju. Ja kaut viens no minētajiem komponentiem nesakrīt, PIN ievades iekārtu ekspluatēt nedrīkst.

First Data.

5. Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei III

Pirms iegādāties PIN ievades iekārtu, rekomendējam pārbaudīt šīs iekārtas lietojuma derīguma termiņu.

PIN ievades iekārtas standarta versija, pret kuru iekārta ir sertificēta	Sertifikācijas derīguma termiņš	Ekspluatācijas beigu termiņš**
1.x	2014. gada 30. aprīlis*	Pašlaik nav noteikts
2.x	2017. gada 30. aprīlis*	Pašlaik nav noteikts
3.x	2020. gada 30. aprīlis*	Pašlaik nav noteikts
Pre-PCI***	2007. gada 31. decembris*	2012. gada 31. decembris****
Visas pārējās iekārtas	–	2010. gada 30. jūnijs****

** https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html*

*** PCI standartam atbilstošo iekārtu ekspluatācijas beigu termiņu nosaka starptautiskās maksājumu karšu organizācijas.*

**** Iekārtas, kuras neatbilst PCI standartam, bet kuru izmantošanu apstiprinājušas starptautiskās maksājumu karšu organizācijas.*

***** http://www.sepalatvija.lv/sites/default/files/20100506_Par_VISA_MC_parmainaam.pdf*

First Data.

5. Ieteikumi viedkaršu pieņemšanas un PIN ievades iekārtu iegādei IV

- Ja uzņēmumā plānots izmantot PIN kodu kā kartes lietotāja pārbaudi visiem karšu darījumiem (arī kartēm ar magnētisko celiņu), papildus jāievēro šādi aspekti:
  - nešifrēts PIN kods drīkst atrasties tikai drošā fiziskā iekārtā (*Tamper Resistant Security Module*; TRSM);
  - iekārtām, kas veic PIN transakciju šifrēšanu (*Hardware Security Module;* HSM) jāatbilst *FIPS 140.2 Level 3* standartam;
  - PIN kods ārpus drošās iekārtas obligāti jāšifrē, izmantojot *TripleDES* šifrēšanas algoritmu.
- Videonovērošanas iekārtām jābūt orientētām tā, lai ierakstā nebūtu redzama ne PIN koda ievades tastatūra, ne arī tas, kā kartes lietotājs ievada PIN kodu.

First Data.

Jautājumi?

Paldies par uzmanību!

First Data.