HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Payment Card Industry Data Security Standard

CCERT-PUBDOC-2006-09-168

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Danas među organizacijama koje posluju s kreditnim karticama postoji velika potreba za podizanjem razine računalne sigurnosti jer u suprotnom efekti mogu biti pogubni po organizaciju. Moguće štete krađe kartica za organizacije koje posluju s njima su:

- gubitak ugleda,
- gubitak klijenata – kupaca te
- gubitak profita.

U početcima su između kreditnih organizacija postojale rasprave na koji način se trebaju zaštititi podaci s kreditnih kartica. Različite kreditne organizacije su primjenjivale i zahtijevale različite sigurnosne politike što je uzrokovalo zbrku među organizacijama koje su poslovale s kreditnim karticama jer nisu znali koji standard moraju slijediti. Kako bi zadovoljili svoje članove, prodavače i posredne pružatelje usluga poslovanja kreditnim karticama, koji su zahtijevali jedinstveni pristup informacijskoj sigurnosti za sve korištene kreditne kartice, vodeće kreditne organizacije (Visa, MasterCard, Japan Central Bank, American Express) su se u prosincu 2004. usuglasile u kreiranju jedinstvenog industrijskog sigurnosnog standarda koji je poznatiji kao *Payment Card Industry (PCI) Data Security Standard*. Od tada se od svih organizacija koje pohranjuju informacije s kreditnih kartica, obrađuju ih ili ih prenose, zahtjeva usklađenost s novim standardom. Novi standard sastoji se od dvanaest detaljno objašnjenih zahtjeva koja su podijeljena u šest kategorija:

1. izgradnja i održavanje sigurne računalne mreže,
2. zaštita kartičnih informacija,
3. održavanje i razvijanje sigurnosnog upravljačkog programa,
4. implementiranje snažnih pristupnih kontrola,
5. konstantni nadzor i testiranje mreže i
6. održavanje i razvijanje sigurnosnih informacijskih politika.

Dodatno, sigurnosni zahtjevi koji se primjenjuju na organizacije, moraju se primjenjivati i na sve sistemske komponente koje su definirane kao mrežne komponente, poslužitelji ili aplikacije, koje su uključene ili sudjeluju u procesuiranju informacija s kreditnih kartica. Mrežne komponente uključuju prije svih i ove uređaje: vatrozidi, preklopnici, usmjerivači, WAP (eng. *Wireless Application Protocol*) pristupne točke, poslužitelji, itd... Poslužitelji mogu biti neki od sljedećih: HTTP, baze podataka, autentikacijski poslužitelj, DNS (eng. *Domain Name Server*) poslužitelj, poslužitelj za elektroničku poštu, posredni poslužitelji (eng. *proxy*), NTP (eng. *Network Time Protocol*), itd... Aplikacije na koje se moraju primjenjivati sigurnosni zahtjevi, uključuju sve oblike razvijanih aplikacije uključujući i unutarnje i eksterne (web) aplikacije.

U ovom dokumentu su opisani osnovni oblici mogućih krađa informacija s kreditnih kartica. Također, opisani su i sigurnosni zahtjevi koje propisuje PCI DSS standard.

2. Opasnosti krađe kartičnih podataka

Opće je poznato da se krađe kartičnih podataka događaju svakodnevno. Pri tome se krađe mogu izvršavati u dvije glavne varijante:

- krađa od korisnika i
- krađa od kartičnih organizacija ili posrednika.

2.1. Krađa kartičnih podataka od korisnika

Krađa kartičnih podatka od korisnika se može ostvariti krađom same kartice ili krađom podataka s kartice. Krađa same kartice nije toliko česta pojava uglavnom zato što korisnici brzo primijete nestanak kartice te ona, pravovremenom reakcijom korisnika i kartične organizacije, u kratkom roku postaje nevažeća. Posljedica toga je da su štete nastale krađom kartica uglavnom ograničene na manje iznose počinjene u kratkom vremenu koje protekne od krađe pa do onesposobljavanja kartice. Uz sve veću upotrebu autorizacije kartičnih transakcija na prodajnim mjestima u stvarnom vremenu, šteta počinjena na ovaj način je minimalna.
Krađa kartičnih podataka bez krađe kartica je nešto opasniji način krađe jer može proteći neko vrijeme dok korisnik i kartična organizacija shvate da je do krađe uopće došlo – obično je to vrijeme od krađe pa do slanja/primitka izvješća o učinjenim troškovima koje se u većini slučajeva šalje na mjesečnoj bazi. Krađa samih podataka se može obaviti na više načina:

- provlačenjem kartice kroz lažni uređaj (eng. *skimming*),
- neovlaštenim uvidom u podatke nezaštićene kartice,
- krađa kartičnih podataka u elektroničkom obliku,
- krađa obmanom (eng. *phishing*), itd.

2.1.1. Krađe provlačenjem kartice kroz lažni uređaj

Skimming je termin koji se upotrebljava za opis krađe kartičnih podataka provlačenjem kartice kroz lažni uređaj za naplatu. Takav oblik krađe uglavnom se dešava na prodajnim mjestima gdje korisnik daje svoju karticu trgovcu prilikom plaćanja, a ovaj to zlorabi te osim što provuče karticu kroz važeći uređaj za naplatu, karticu provlači i kroz lažni uređaj te tako dolazi u posjed podataka s kartice. Korisnik obično nije svjestan krađe dok naknadno ne utvrdi neovlašteno korištenje kartice.
Treba spomenuti i pojavu *skimming* prevare na bankomatima gdje su maliciozni napadači instalirali lažni uređaj za čitanje kartica ispred otvora za karticu na bankomatu tako da kartica prilikom ubacivanja u bankomat prolazi i kroz lažni uređaj koji s nje očitava podatke. Jedinstveni PIN se pri tome detektira korištenjem minijaturnih video kamera.
Iako je ovakav oblik krađe kartičnih podataka dosta raširen, broj krađa se ipak smanjuje zbog uvođenja pametnih kartica, tj. kartica koje uz magnetski zapis imaju i mikročip kao dodatni sigurnosni mehanizam. Pošto podatke s mikročipa nije jednostavno pročitati, a ti podaci su nužni za sigurnosne provjere kartica, to će u budućnosti uz povećanje broja prikladnih kartičnih terminala znatno smanjiti ovaj oblik krađe kartičnih podataka.

2.1.2. Neovlašteni uvid u podatke nezaštićene kartice

Korisnici često smetnu s uma da napadač ne mora nužno ukrasti karticu da bi iskoristio podatke s iste. Dovoljno je karticu ostaviti nepokrivenu na stolu u uredu da netko s nje pročita podatke i iste iskoristi. U većini slučajeva podaci samo s prednje strane kartice neće biti dovoljni jer se kod plaćanja uglavnom traži kontrolni broj otisnut na poleđini kartice, ali ako se omogući i uvid u drugu stranu kartice, ta vrsta zaštite nestaje. Zbog toga se preporuča korisnicima da budu pažljivi u rukovanju s kreditnim karticama i spriječe ovakav trivijalan oblik krađe.

2.1.3. Krađa kartičnih podataka u elektroničkom obliku

S porastom upotrebe elektroničkog plaćanja putem Interneta, porasla je i količina krađa kartičnih podataka u elektroničkom obliku koji se izmjenjuju putem elektroničkih platnih transakcija. Krađa podataka u elektroničkom obliku može se obaviti na više načina i na više mjesta:

- krađa praćenjem mrežnog prometa,
- krađa web kolačića,
- krađa upadom na korisnikovo računalo, itd.

Krađa praćenjem mrežnog prometa ostvaruje se tzv. „*sniffing*" procesom, tj. prisluškivanjem prometa na određenom komunikacijskom kanalu. Posebnim alatima, prisluškivani promet koji obično uključuje više kanala i korisnika, može se razložiti na pojedine kanale i korisnike, te se tada može dešifrirati dio ili cjelokupan sadržaj komunikacije. Ovakav oblik krađe je vrlo rijedak zbog činjenice da je količina prometa koja se razmjenjuje komunikacijskim kanalima ogromna pa je proces razlaganja ukupnog prometa na pojedine korisnike praktički nemoguć zbog prevelikih procesorskih zahtjeva potrebnih za takvu operaciju. Uz to, većina današnjih platnih transakcija obavlja se zaštićenim kanalima (SSL ili slični sigurnosni protokol) što dodatno otežava dešifriranje informacija čak i kad bi se razlaganje prometa moglo uspješno obaviti.

Krađa web kolačića je češći oblik krađe kartičnih podataka. Naime, web kolačići se koriste za pohranjivanje i prijenos korisničkih podataka od korisnika do web poslužitelja, te kao takvi oni često između ostalih podataka sadrže i kartične podatke. Web kolačići se mogu krasti praćenjem prometa, ali je taj način krađe iz gore navedenih razloga vrlo rijedak. Češći način krađe je pomoću tzv. „*cross site scripting*" (XSS) napada gdje se korisnikovi web kolačići pomoću malicioznih skripti preusmjeravaju s web poslužitelja za koji su predviđeni na web poslužitelj malicioznog napadača. Napad se zasniva na izvršavanju malicioznih skripti unutar korisnikovog web preglednika ili unutar samog web poslužitelja, koje omogućavaju sigurnosni propusti korisnikovog web preglednika ili web poslužitelja za koji su kolačići predviđeni. Za zaštitu od takvih napada potrebno je na strani web preglednika podesiti sigurnosne postavke tako da se onemogući izvršavanje skripti, a na strani web poslužitelja ograničiti upotrebu skripti i obavljati validaciju unosa podataka i skripti koje se moraju koristiti.

Krađa upadom na korisnikovo računalo je također čest način krađe kartičnih podataka koji se obavlja ciljanim hakerskim napadom pri čemu se koriste sigurnosni propusti u konfiguraciji korisnikovog računala koji omogućavaju neovlašteno izvršavanje proizvoljnog koda na korisnikovom računalu kojim se korisnički podaci šalju napadaču. Zaštitu od takvih napada pružaju vatrozidi, te redovito instaliranje sigurnosnih zakrpa za aplikacije koje su na računalu instalirane, a koje se spajaju na Internet.

2.1.4. Krađa obmanom

Krađa obmanom (eng. *phishing*) je postao popularan način krađe kartičnih podataka jer ne zahtijeva veliku tehničku stručnost već se bazira na lakovjernosti i nepažnji korisnika. *Phishing* napad se ostvaruje lažiranjem identiteta, tj. lažnim korištenjem identiteta povjerljive osobe ili web poslužitelja kako bi se ponukalo korisnika da sam otkrije povjerljive podatke. *Phishing* napad se obično realizira putem poruka elektroničke pošte ili tzv. trenutnim porukama (eng. *instant messages*) koje izgledaju kao da su došle od kartične organizacije, ali sadrže URL-ove koji nemaju veze s kartičnom organizacijom ili zahtijevaju od korisnika slanje poruka s kartičnim podacima na neku adresu. Ukoliko korisnik povjeruje danom zahtjevu, poruka s podacima odlazi malicioznim napadačima. Isto tako, ako korisnik klikne na zlonamjerno prilagođeni URL, korisnikov zahtjev se preusmjerava na maliciozni web poslužitelj putem kojeg će se malicioznim skriptama ukrasti njegovi kartični podaci. Zaštitu od ovakvih napada u najvećem broju slučajeva mogu osigurati sami korisnici pažljivim čitanjem i provjeravanjem dobivenih poruka.

2.2. Krađa kartičnih podataka od kartičnih organizacija ili posrednika

Krađa podataka od kartičnih organizacija je drugi način krađe kartičnih podataka koji obično završi s težim posljedicama jer se prilikom krađe napadač domogne kartičnih podataka ne jednog nego velikog broja korisnika. Takvi se napadi uglavnom realiziraju probojem u računalni sustav kartičnih organizacija ili njihovih posrednika i to iskorištavanjem nekog sigurnosnog propusta.

Da bi spriječile takve napade, kartične organizacije inzistiraju na provođenju striktnih sigurnosnih procedura unutar svojih podružnica, ali i svojih posrednika. Međutim, zbog velikog broja posrednika (trgovine koje omogućavaju plaćanje karticama) i nemogućnosti potpunog nadzora nad sigurnosnim uvjetima na lokacijama posrednika, takvi napadi nisu rijetkost.

Radi smanjenja takvih pojava i uspostave veće homogenosti sigurnosnih uvjeta na cijelom području mreže kartičnog poslovanja, kartične organizacije usvojile su i nalažu svim podružnicama i posrednicima primjenu standarda o sigurnosti podataka u kartičnom poslovanju – *Payment Card Industry Data Security Standard*. Sadržaj tog standarda predmet je nastavka ovog dokumenta.

3. Payment Card Industry Data Security Standard

PCI DSS sigurnosni standard se primjenjuje na sve članove, trgovce i pružatelje usluga koji su povezani sa spremanjem, procesuiranjem i prosljeđivanjem informacija s kreditnih kartica. Dodatno, ti sigurnosni zahtjevi se primjenjuju na sve sigurnosne elemente koji su uključeni u elektroničko poslovanje povezano s kreditnim karticama.

Organizacije na koje se primjenjuju definirana pravila, podijeljene su u četiri različite kategorije:

- privrednici (trgovci) prve razine – one organizacije koje ostvaruju preko 6 milijuna kartičnih transakcija godišnje,
- privrednici (trgovci) druge razine – one organizacije koje ostvaruju od 150 tisuća do 6 milijuna kartičnih transakcija godišnje,
- privrednici (trgovci) treće razine – one organizacije koje ostvaruju od 20 do 150 tisuća kartičnih transakcija godišnje,
- privrednici (trgovci) četvrte razine – one organizacije koje ne spadaju u prethodno navedene kategorije.

Na prethodno navedene kategorije organizacija primjenjuju se različiti oblici zahtjeva počevši od obaveznih kvartalnih analiza koje provode nepristrani sigurnosni stručnjaci, do preporučenih godišnjih analiza koje organizacije mogu same provesti.

U nastavku ovog poglavlja opisano je dvanaest sigurnosnih zahtjeva koji su podijeljeni u šest kategorija.

3.1. Izgradnja i održavanje sigurne računalne mreže

Prva kategorija sigurnosnih zahtjeva koji se primjenjuju na organizacije koje sudjeluju u poslovanju s kreditnim karticama je osiguranje izgradnje i održavanja sigurne računalne mreže. Za tu svrhu neophodni su mrežni vatrozidi. Mrežni vatrozidi su takvi uređaji koji kontroliraju mrežni promet koji dolazi u organizaciju kao i mrežni promet koji napušta organizaciju. Pri tomu određene komponente unutarnje mreže mogu imati različite nivoe sigurnosne zaštite – neki su manje, a neki više zaštićeni. Svi sustavi trebaju biti zaštićeni od neautoriziranih pristupa s Interneta, kako za elektroničko poslovanje, tako i za zaposleničke pristupe izvana te njihove pristupe elektroničkoj pošti. Tu zaštitu je djelomično teško ostvariti pošto u organizacijama znadu postojati i naizgled beznačajni putovi na i s Interneta koji mogu omogućiti nezaštićeni pristup u ključne elemente sustava. Vatrozidi su stoga nužni jer predstavljaju ključni zaštitni mehanizam za svaku računalnu mrežu.

3.1.1. Instaliranje i održavanje vatrozidove konfiguracije u svrhu zaštite podataka

Ovo poglavlje specificira konfiguraciju vatrozida i pripadnih sigurnosnih procedura zahtijevanih standardom. Prema standardu potrebno je sljedeće:

1. Uspostaviti konfiguraciju vatrozidnih standarda što uključuje:
    a. formalni proces za odobravanje i testiranje svih eksternih mrežnih veza i promjena u konfiguraciji vatrozida,
    b. trenutno aktivni mrežni dijagram sa svim vezama prema kartičnim podacima uključujući i bežične veze,
    c. obavezu postojanja vatrozida na svakoj vezi prema Internetu i između de-militarizirane zone (DMZ) i Interneta,
    d. opis grupa, uloga i odgovornosti za logičko upravljanje mrežnim komponentama,
    e. dokumentirani popis svih servisa i portova koji su zahtijevani za poslovanje,
    f. opravdanje i dokumentaciju za sve dostupne protokole povrh HTTP, SSL, SSH, i VPN protokola,

g. opravdanje i dokumentaciju za eventualne dozvoljene riskantne protokole (npr. FTP protokol) što uključuje specifikaciju razloga za korištenje protokola i implementiranih sigurnosnih mehanizama,
h. periodične preglede svih konfiguriranih pravila na vatrozidima i usmjerivačima i
i. konfiguracijske standarde za usmjerivače.

2. Uspostaviti konfiguraciju vatrozida koja onemogućava sav promet od i prema „nepovjerljivim" mrežama i poslužiteljima osim za:
   a. web protokole – HTTP (port 80) i SSL (uobičajeno port 443),
   b. protokole za sistemsku administraciju (npr. SSH ili VPN protokol),
   c. ostale protokole potrebne za poslovanje (npr. za ISO 8583).
3. Uspostaviti konfiguraciju vatrozida koja ograničava veze prema javno dostupnim poslužiteljima i komponentama sustava koje se koriste za pohranjivanje kartičnih podataka uključujući i bežične veze. Konfiguracija treba uključivati:
   a. ograničenje dolaznog Internet prometa na IP adrese unutar DMZ-a koja uobičajeno predstavlja odvojenu mrežu poslužitelja,
   b. ograničenje dolaznog i odlaznog Internet prometa na HTTP i SSL portove (80 i 443),
   c. zabraniti prolazak mrežnih paketa koji imaju postavljenu kao izvornu IP adresu iz unutarnje mreže, a koji su usmjereni na DMZ,
   d. dinamičko filtriranje paketa (eng. *stateful inspection*) prema kojem se s Interneta na unutarnju mrežu dozvoljava prolazak samo onih paketa koji su dio uspostavljenih veza (samo računala iz unutarnje mreže mogu uspostavljati konekcije),
   e. postavljanje baze podataka u unutarnju mrežu koja mora biti odvojena od DMZ-a,
   f. ograničavanje odlaznog prometa na minimum koji je potreban za ostvarivanje kartičnog poslovanja,
   g. osiguravanje i sinkroniziranje konfiguracijskih datoteka usmjerivača (npr. konfiguracijske datoteke za normalni rad i konfiguracijske datoteke koje se koriste kod podizanja sustava, moraju se izvršavati pod istom sigurnosnom konfiguracijom),
   h. onemogućavanje svog dolaznog i odlaznog prometa koji nije posebno dozvoljen,
   i. instalacija graničnih vatrozida između bežičnih mreža i okruženja za plaćanje karticama; konfiguracija tih vatrozida mora biti takva da onemogući ili ograniči promet s bežičnim mrežama ako je takav promet potreban za poslovanje,
   j. instalacija vatrozida na sve mobilne uređaje i osobna računala zaposlenika ukoliko takva računala imaju direktan pristup Internetu i koriste se za pristup organizacijskoj mreži.
4. Zabraniti direktan javni pristup komponentama sustava na kojem se pohranjuju kartični podaci (npr. baze podataka) iz vanjskih mreža:
   a. implementirati DMZ za filtriranje i nadzor svog prometa te za zabranu svih direktnih odlaznih i dolaznih ruta prema Internetu, i
   b. ograničiti odlazni promet od kartičnih aplikacija na IP adrese unutar DMZ-a.
5. Implementirati IP maskiranje kako bi se spriječilo prevođenje i otkrivanje IP adresa na Internetu. Koristiti tehnologije koje implementiraju RFC 1918 adresni prostor kao što je prepisivanje portova - PAT (eng. *Port Address Translation*) i IP adresa - NAT (eng. *Network Address Translation*)

3.1.2. Izbjegavanje korištenja proizvođačevih predefiniranih sistemskih zaporki i ostalih sigurnosnih parametara

Udaljeni i lokalni napadači i zlonamjerni korisnici često koriste predefinirane zaporke podešene od strane proizvođača mrežne opreme kako bi kompromitirali sustav. Te zaporke su vrlo dobro znane na hakerskoj sceni i lako dostupne putem javnih resursa.

Zbog toga je potrebno osigurati određene sigurnosne elemente:

1. Uvijek promijeniti predefinirane postavke dostavljene od strane proizvođača mrežne opreme prije nego što se sustav priključi na mrežu (npr. zaporke i predefinirani nepotrebni korisnički računi):

   a. za bežična okruženja promijeniti predefinirane postavke proizvođača opreme između ostalog uključujući i WEP (eng. *Wireless Equivalent Privacy*) ključeve, predefinirane identifikatore za bežični pristup - SSID (eng. *Service Set Identifier*), zaporke i SNMP jedinstvene oznake – zaporke (eng. *community strings*), te onemogućiti razašiljanje (eng. *broadcast*) SSID oznaka bežične mreže. Omogućiti WPA (eng. *Wi-Fi Protected Access*) tehnologiju za enkripciju i autentikaciju ako oprema posjeduje podršku za WPA tehnologiju.
2. Razviti konfiguracijske standarde za sve komponente sustava. Pobrinuti se da ti standardi obuhvaćaju sve poznate sigurnosne ranjivosti i industrijski prihvaćene najbolje prakse:
   a. implementirati samo jednu primarnu funkciju po poslužitelju (npr. web i DNS poslužitelji trebaju biti implementirati na odvojenim računalima),
   b. isključiti sve nepotrebne i nesigurne usluge i protokole (usluge i protokole koji nisu nužno potrebni za obavljanje tražene funkcije),
   c. konfigurirati sigurnosne parametre sustava tako da se spriječe zlouporabe,
   d. maknuti sve nepotrebne funkcionalnosti kao što su skripte, upravljački/pogonski programi, dodatne funkcionalnosti, podsustave, dijeljene sustave (npr. nepotrebne web poslužitelje).
3. Kriptirati sav administrativni pristup koji nije preko komandne linije. Koristiti tehnologije kao što su SSH, VPN ili SSL/TLS za web bazirano upravljanje i ostali administrativni pristup koji nije preko komandne linije.

3.2. Zaštita kartičnih podataka

Enkripcija je finalni zaštitni mehanizam jer čak i ako netko probije sve ostale sigurnosne mehanizme i dobije pristup kriptiranim podacima, te podatke neće moći iskoristiti bez razbijanja enkripcije.

3.2.1. Zaštita pohranjenih podataka

Radi zaštite pohranjenih podataka potrebno je sljedeće:

1. Pohranjivati minimalno potrebnu količinu podataka o kreditnim karticama. Razviti politike i procedure za zadržavanje potrebnih i odlaganje nepotrebnih podataka. Ograničiti količinu podataka i vrijeme zadržavanja podataka na ono koje je potrebno za poslovanje, određeno pravnim regulativama ili politikama za zadržavanje podataka.
2. Izbjegavati pohranjivanje osjetljivih autentikacijskih podataka nakon autorizacije (čak ni u kriptiranom obliku):
   a. izbjegavati pohranjivanje punog sadržaja bilo kojeg retka zapisa s magnetske trake (s pozadine kartice, s mikročipa, itd.),
   b. izbjegavati pohranjivanje validacijskog koda kartice (eng. CVC – *Card Validation Code*) – troznamenkasti ili četveroznamenkasti broj otisnut na prednjoj ili zadnjoj strani kartice (npr. CVV2 ili CVC2 broj),
   c. izbjegavati pohranjivanje PIN koda kartice (eng. PVV – *Pin Verification Value*).
3. Maskirati brojeve računa prilikom prikaza (maksimalno prvih 6 i zadnje 4 znamenke smiju biti prikazane). Ipak, ovaj zahtjev se ne odnosi na one djelatnike i druge stranke koji imaju specifičnu potrebu za uvidom u kompletan broj kreditne kartice.
4. Pretvoriti osjetljive kartične podatke u nečitljiv oblik na svim mjestima pohrane (uključujući i prijenosne medije, medije za pohranu sigurnosnih kopija, log datoteke, dolazne i odlazne podatke prema bežičnim mrežama) korištenjem jedne od navedenih metoda:
   a. jednosmjerni sažetak (eng. *One-way hash*) kao što je SHA-1,
   b. skraćivanje (eng. *Truncation*),
   c. indeks tokeni i uređaji za generiranje zaporki koji rade na principu generiranja različitih zaporki u različito vrijeme,
   d. jaka kriptografija kao što je 128-bitni 3DES (trostruki DES - *Data Encryption Standard*) ili 256-bitni AES (eng. *Advanced Encryption Standard*) s prikladnim procedurama i politikama za upravljanje ključevima.

   Minimum podataka koji mora biti nečitljiv je broj kartice.
5. Zaštititi enkripcijske ključeve od otkrivanja i zlouporaba:

a. ograničiti pristup ključevima na minimalan broj osoba zaduženih za održavanje,
b. sigurno pohraniti ključeve na što manji broj lokacija i u što manjem broju formata.

6. Dokumentirati i implementirati sve procedure upravljanja ključevima koje uključuju:
   a. generiranje jakih ključeva,
   b. sigurnu distribuciju ključeva,
   c. sigurno pohranjivanje ključeva,
   d. periodične izmjene ključeva,
   e. uništavanje starih ključeva,
   f. podjela znanja i dualna kontrola ključeva (tako da su potrebne 2 ili 3 osobe od kojih svaka zna dio ključa da bi se rekonstruirao ključ),
   g. zaštitu od neautorizirane zamjene ključeva,
   h. zamjenu dokazano kompromitiranih ključeva ili onih za koje se sumnja da su kompromitirani,
   i. opoziv starih i nevažećih ključeva (uglavnom za RSA ključeve),
   j. obaveza potpisivanja formulara kojim odgovorna osoba prihvaća odgovornosti za održavanje ključeva.

3.2.2. Kriptiranje prijenosa kartičnih informacija i ostalih povjerljivih informacija preko računalnih mreža

Osjetljivi podaci moraju biti kriptirani kad se prenose putem Interneta kako bi se potencijalnim napadačima onemogućilo presretanje i preusmjeravanje podatka tijekom prijenosa. Zbog toga je potrebno sljedeće:

1. Koristiti jaku kriptografiju i kriptografske mehanizme (minimum 128-bitne) kao što su SSL, PPTP (eng. *Point-To-Point Tunnelling Protocol*), IPSec (eng. *Internet Protocol Security*) za zaštitu osjetljivih kartičnih podataka tijekom prijenosa putem javnih mreža:
   a. kod prijenosa kartičnih podataka bežičnim mrežama potrebno je kriptirati podatke korištenjem WPA (eng. *Wi-Fi Protected Access*) tehnologijom ako je dostupna ili koristiti VPN ili SSL 128-bitnu zaštitu; nikada se za zaštitu podataka ne smije koristiti samo WEP (eng. *Wired Equivalent Privacy*), a navedene metode zaštite se moraju koristiti uz 128-bitni WEP, a uz to je potrebno rotirati dijeljene WEP ključeve svaka 3 mjeseca kao i kod promjene osoblja,
   b. nikada se ne smiju slati kartični podaci putem nekriptiranih poruka elektroničke pošte.

3.3. Održavanje i razvijanje sigurnosnog upravljačkog programa

Velik broj ranjivosti i malicioznih programa u mrežu dolazi posredstvom zaposlenika i njihovih poruka elektroničke pošte. Na svim sustavima elektroničke pošte i radnim stanicama potrebno je koristiti antivirusnu zaštitu protiv malicioznih programa.

3.3.1. Korištenje i redovito nadograđivanje anti-virusnih programa

U svrhu zaštite od različitih oblika malicioznih programa potrebno je;

1. instalirati antivirusne mehanizme na sve sustave podložne virusima (npr. osobna računala i poslužitelji) i
2. voditi brigu o tome da su svi antivirusni sustavi aktivni, opremljeni najnovijim virusnim definicijama te da su sposobni generirati log zapise.

3.3.2. Razvijanje i održavanje sigurnih sustava i aplikacija

Beskrupulozni pojedinci koriste sigurnosne ranjivosti radi dobivanja privilegiranog pristupa zaštićenim sustavima. Velik broj ovih ranjivosti može se popraviti sigurnosnim zakrpama koje osigurava proizvođač opreme/sustava pa je potrebno voditi brigu o tome da se na sve sustave instaliraju najnovije verzije zakrpa kako bi se osigurala zaštita od potencijalnih napadača bilo zaposlenika, udaljenih napadača ili malicioznih programa. Što se tiče internih aplikacija razvijenih

unutar organizacije, ranjivosti je potrebno izbjegavati upotrebom standardnih procedura razvoja programa i sigurnosnih tehnika kodiranja. Kako bi se gore navedeno ostvarilo, potrebno je:

1. Osigurati da su sve komponente sustava opremljene najnovijim verzijama sigurnosnih zakrpa:
    a. potrebno je instalirati relevantne zakrpe najkasnije mjesec dana nakon izdavanja.
2. Uspostaviti procese za otkrivanje novih sigurnosnih ranjivosti (npr. pretplatiti se na usluge obavještavanja o sigurnosnim prijetnjama dostupnim na Internetu). Obnavljati vlastite standarde da obuhvate najnovije sigurnosne prijetnje.
3. Razvijati vlastite aplikacije u skladu s najboljim industrijskim praksama te uključiti sigurnosne procedure u proces razvoja programa. Procedure uključuju sljedeće:
    a. testiranje svih sigurnosnih zakrpa i konfiguracijskih promjena prije puštanja u upotrebu,
    b. odvojiti okruženja za razvoj/testiranje od produkcijskog okruženja,
    c. odvojiti razvojno/testna zaduženja od produkcijskih zaduženja,
    d. produkcijski podaci (stvarni brojevi kreditnih kartica) ne smiju se koristiti za razvoj/testiranje,
    e. testni podaci i brojevi kartica moraju se izbrisati prije aktiviranja produkcijskih sustava,
    f. radni korisnički računi i zaporke moraju se izbrisati prije davanja aplikacije na upotrebu stvarnim klijentima,
    g. revidirati novo proizvedeni kod prije puštanja aplikacija u produkciju radi identifikacije potencijalnih sigurnosnih ranjivosti.
4. Pridržavati se procedura za kontrolu izmjena kod bilo kakvih izmjena sustava ili konfiguracije sustava. Procedure uključuju:
    a. dokumentiranje utjecaja izmjene,
    b. potpisivanje od strane odgovornog menadžmenta,
    c. testiranje operativne funkcionalnosti,
    d. procedure za povlačenje izmjene.
5. Razvijati web programe prema uputama za sigurno kodiranje kao što su *Open Web Application Security Project Guidelines* [3]. Revidirati kod razvijene aplikacije radi detekcije sigurnosnih ranjivosti. Izbjeći sljedeće najčešće ranjivosti uzrokovane greškama u procesu razvoja programa:
    a. nevalidirani unos,
    b. neovlašten pristup (npr. maliciozno korištenje korisničkog identiteta),
    c. neovlaštena autentikacija / upravljanje sesijama (korištenje korisničkih podataka ili kolačića sesije),
    d. *Cross site scripting* (XSS) napadi,
    e. prepisivanje spremnika,
    f. ugnježđivanje naredbi (npr. SQL naredbi),
    g. nepravilna obrada greški,
    h. nesigurno pohranjivanje,
    i. uskraćivanje usluge,
    j. nesigurno upravljanje konfiguracijom.

3.4. Implementiranje snažnih pristupnih kontrola

Preporuke opisane u nastavku služe za osiguravanje autoriziranog pristupa kritičnim podacima.

3.4.1. Zaštita pristupa podacima prema načelu dozvoljenog pristupa onima koji moraju znati

Za ostvarenje zaštite potrebno je:

1. ograničiti pristup računalnim resursima i kartičnim podacima samo na osobe čiji posao i zaduženja to zahtijevaju,
2. implementirati mehanizme za sustave s više korisnika koji će ograničiti pristup prema potrebama i koji kreće od inicijalnog ograničenja „zabrani sve“ osim ako nije drugačije specificirano.

3.4.2. Pridjeljivanje jedinstvenog identifikatora svakoj osobi s računalnim pristupom

Da bi se osigurala mogućnost praćenja aktivnosti nad kritičnim podacima i resursima potrebno je:

1. Identificirati svakog korisnika jedinstvenim identifikatorom prije odobrenja pristupa.
2. Povrh identifikacije koristiti barem jednu od navedenih metoda autentikacije:
    a. zaporka,
    b. token uređaji (npr. identifikatori, certifikat, javni ključ),
    c. biometrijski podaci.
3. Implementirati autentikaciju s dva faktora za udaljeni pristup mreži za djelatnike, administratore i treće stranke. Koristiti tehnologije kao što su RADIUS (eng. *Remote Authentication Dial-In User Service*) ili TACACS (eng. *Terminal Access Controller Access Control System*) korištenjem tokena ili individualnih certifikata.
4. Kriptirati sve zaporke prilikom prijenosa ili pohrane na svim komponentama sustava.
5. Osigurati pravilnu autentikaciju korisnika i upravljanje zaporkama za netipične korisnike i administratore na svim komponentama sustava:
    a. kontrolirati kreiranje, brisanje i modifikaciju korisničkih identiteta, podataka i drugih identifikacijskih objekata,
    b. verificirati korisničke identitete prije re-izdavanja zaporki,
    c. koristiti jedinstvenu inicijalnu zaporku za svakog korisnika i inzistirati na obaveznoj promjeni nakon prve upotrebe,
    d. odmah opozvati prava pristupa za opozvane korisnike,
    e. izbrisati neaktivne korisnike barem svakih 90 dana,
    f. omogućiti prava udaljene administracije za proizvođače opreme samo za vrijeme kad je to potrebno,
    g. distribuirati procedure upravljanja zaporkama svim korisnicima koji imaju pravo pristupa kartičnim podacima,
    h. ne koristiti grupne, dijeljene ili generičke zaporke i korisničke račune,
    i. mijenjati korisničke zaporke barem svakih 90 dana,
    j. zahtijevati minimalnu dužinu zaporke od 7 znakova,
    k. koristiti zaporke koje sadrže i brojke i slova,
    l. ne dozvoliti upotrebu nove zaporke ako je ona identična nekoj od zadnje 4 korištene,
    m. ograničiti ponavljanje autentikacije na maksimalno 6 puta nakon čega se upotrijebljeni korisnički račun blokira,
    n. podesiti trajanje blokade korisničkog računa na 30 minuta ili dok administrator ne obavi ručno deblokiranje,
    o. ako je sesija neaktivna duže od 15 minuta, zahtijevati ponovni unos zaporke za re-aktivaciju terminala,
    p. autenticirati svaki pristup bazama podataka koje sadrže kartične podatke što uključuje pristup aplikacija, administratora i drugih korisnika.

3.4.3. Ograničavanje fizičkog pristupa kartičnim informacijama

Svaki fizički pristup kartičnim podacima ili sustavu na kojem su ti podaci pohranjeni predstavlja priliku za krađu tih podataka pa ga treba strogo ograničiti što podrazumijeva sljedeće:

1. Koristiti prikladne mehanizme kontrole ulaza za ograničavanje i nadzor fizičkog pristupa sustavima za pohranjivanje, prijenos ili obradu kartičnih podataka
    a. koristiti kamere za nadzor osjetljivih područja uz što je potrebno pregledavati snimke kamera te ih korelirati s ostalim podacima; snimke je potrebno pohranjivati najmanje 3 mjeseca osim ako ne postoje drugačija zakonska ograničenja,
    b. ograničiti fizički pristup javno dostupnim mrežnim priključcima,
    c. ograničiti fizički pristup bežičnim pristupnim točkama, poveznicima ili prijenosnim terminalima.
2. Razviti procedure kojima će se olakšati razlikovanje zaposlenika i posjetioca u područjima gdje su kartični podaci dostupni.

Termin „zaposlenik“ podrazumijeva djelatnike s punim ili djelomičnim radnim vremenom, privremene djelatnike i konzultante koji su stalni na toj lokaciji. Termin „posjetilac“ podrazumijeva proizvođača opreme, servisno osoblje, goste zaposlenika ili bilo koju drugu osobu koja ulazi u zaštićeni prostor na kraći period, obično ne duže od jednog dana.

3. Osigurati da su svi posjetioci:
    a. autorizirani prije ulaska u prostor gdje se pohranjuju ili obrađuju kartični podaci,
    b. opskrbljeni fizičkim tokenom (npr. bedž ili kartica) koje nije trajna i koja ih identificira kao posjetioce,
    c. kontrolirati predaju dobivenih tokena prilikom izlaska ili prestanka važenja tokena.
4. Koristiti dnevnik posjetioca kako bi se zadržao fizički trag posjeta pri čemu je dnevnik potrebno čuvati minimalno 3 mjeseca ukoliko ne postoje drugačija zakonska ograničenja.
5. Pohranjivati sigurnosne kopije podataka na sigurnoj odvojenoj lokaciji koja može biti ili lokacija treće stranke ili komercijalna ustanova za pohranjivanje podataka.
6. Fizički osigurati sve pisane i elektroničke medije za pohranu podataka (npr. računala, elektroničke medije, mrežnu i komunikacijsku opremu, komunikacijske linije, pisane račune i izvještaje, i sl.) koji sadrže kartične podatke.
7. Implementirati striktne kontrole nad internim i eksternim distribuiranjem svih medija koji sadrže kartične podatke:
    a. označiti medije kao povjerljive,
    b. slati medije putem sigurnih kurira ili dostavnih mehanizama koji omogućavaju praćenje transporta.
8. Osigurati potvrdu menadžmenta za svaki prijenos medija izvan zaštićenog područja (posebno ako se prenosi individualnim osobama).
9. Osigurati striktnu kontrolu pohrane i pristupa medijima koji sadrže kartične podatke:
    a. pravilno evidentirati sve medije i osigurati sigurnu pohranu.
10. Uništiti sve medije koji sadrže kartične podatke, a nisu više potrebni za poslovanje niti zakon zahtijeva njihovo čuvanje:
    a. pisane medije uništiti dvosmjernim rezanjem, spaljivanjem ili prešanjem,
    b. elektroničke medije brisati, de-magnetizirati ili uništiti drugačije tako da se podaci s njih ne mogu rekonstruirati.

3.5. Konstantni nadzor i testiranje mreže

Mehanizmi logiranja i mogućnost praćenja korisničkih aktivnosti su od kritičnog značenja. Prisutnost log zapisa u svim okruženjima omogućava detaljnu analizu neželjenih pojava. Otkrivanje uzroka takvih pojava je vrlo teško ako ne postoje sistemski log zapisi.

3.5.1. Praćenje i registriranje svih pristupa mrežnim resursima i kartičnim informacijama

Praćenje i registriranje pristupa mrežnim resursima i kartičnim informacijama sastoji se od sljedećih elemenata:

1. Uspostaviti proces za povezivanje svih pristupa komponentama sustava s individualnim korisnicima (posebno za pristupe s administrativnim ovlastima – npr. *root* na Unix/Linux sustavima).
2. Uspostaviti automatizirane procedure pregleda log zapisa za rekonstrukciju sljedećih događaja na svim komponentama sustava:
    a. svaki individualni pristup kartičnim podacima,
    b. svaku akciju poduzetu s administrativnim ovlastima,
    c. svaki pristup log zapisima,
    d. pokušaje neuspješnog pristupa,
    e. korištenje identifikacijskih i autentikacijskih mehanizama,
    f. inicijalizacije log zapisa,
    g. kreiranje i brisanje objekta na sistemskom nivou.
3. Zapisivati minimalno sljedeće zapise za svaki događaj na svakoj komponenti sustava:
    a. identitet korisnika,
    b. tip događaja,

   c. datum i vrijeme,
   d. podatak o uspjehu/neuspjehu,
   e. izvor događaja,
   f. identitet ili ime podatka, resursa ili komponente sustava na koji se događaj odnosi.
4. Sinkronizirati sve kritične sistemske satove i vremena.
5. Osigurati log zapise kako se ne bi mogli mijenjati što podrazumijeva sljedeće:
   a. ograničiti prava uvida u log zapise na one osobe čiji posao to zahtijeva,
   b. zaštititi log zapise od neautoriziranih izmjena,
   c. što prije napraviti sigurnosne kopije log zapisa i pohraniti ih na centralni log poslužitelj ili na medij na kojem će ih biti teško izmijeniti,
   d. kopirati log zapise bežičnih mreža na log poslužitelje na internoj mreži,
   e. koristiti alate za detekciju izmjena i kontrolu integriteta datoteka (npr. Tripwire) nad log zapisima kako bi se osiguralo da log zapisi ne mogu biti izmijenjeni bez generiranja alarma (iako dodavanje novih podataka ne bi smjelo generirati alarm).
6. Pregledavati log zapise za sve komponente sustava minimalno na dnevnoj bazi. Pregledi trebaju uključivati poslužitelje odgovorne za detekciju upada (eng. IDS - *Intrusion Detection System*), te poslužitelje za autentikaciju, autorizaciju i obračun (eng. AAA – *Authentication, Authorisation, Accounting*) kao što je npr. RADIUS.
7. Čuvati log zapise u skladu s periodom njihovog korištenja i zakonskim rokovima. Uobičajeni period čuvanja log zapisa je jedna godina s tim da su podaci od zadnja 3 mjeseci dostupni *on-line*.

3.5.2. Regularno testiranje sigurnosnih sustava i procesa

Ranjivosti kontinuirano otkrivaju i dobronamjerni i zlonamjerni istraživači, a pojavljuju se najčešće zajedno s pojavom novih programa. Sustavi, procesi i interne aplikacije trebale bi se redovito testirati kako bi se utvrdilo da li su s vremenom, i usprkos unesenim promjenama, zadržali traženi nivo sigurnosti. Potrebno je:

1. Rutinski testirati sigurnosne kontrole, ograničenja, mrežne veze i ograničenja kako bi se utvrdilo da li pravilno sprečavaju i identificiraju pokušaje neovlaštenog ulaza u sustav. Kod bežičnih mreža potrebno je periodički korištenjem analizatora bežičnih mreža identificirati sve uređaje koji su trenutno u upotrebi.
2. Provoditi interne i eksterne provjere ranjivosti mreže na kvartalnoj bazi i nakon većih izmjena u mreži (npr. nakon instalacije novih komponenti sustava, promjene u topologiji mreže, promjene pravila vatrozida, instalacije zaporki i sl.).
   Eksterne provjere ranjivosti moraju biti provedene od strane stručnjaka kvalificiranih za rad s kartičnim sustavima.
3. Provoditi testiranje proboja (eng. *penetration testing*) mrežne infrastrukture i aplikacija barem jednom godišnje i nakon većih infrastrukturnih promjena (npr. obnavljanje operacijskog sustava, dodavanje pod-mreže, dodavanje web poslužitelja i sl.).
4. Koristiti sustave za detekciju upada u mrežu, lokalne sustave za detekciju upada kao i sustave za detekciju upada na nivou cijele mreže za praćenje cjelokupnog prometa i alarmiranje u slučaju detektiranog sumnjivog događaja. Svi sustavi za detekciju upada moraju biti redovito aktualizirani.
5. Koristiti mehanizme praćenja integriteta podataka za alarmiranje u slučaju neovlaštenih izmjena kritičnih sistemskih datoteka pri čemu je usporedbe kritičnih datoteka potrebno provoditi barem jednom dnevno (ili češće ako je moguće automatizirati proces).
   Kritične datoteke nisu nužno one koje sadrže kartične podatke. Za provjeru integriteta obično je dobro koristiti datoteke koje se ne mijenjaju redovito, ali njihova izmjena može značiti da je sustav kompromitiran. Alati za kontrolu integriteta obično se isporučuju s unaprijed konfiguriranim datotekama koje su kritične za određeni operacijski sustav. Ostale kritične datoteke se moraju pronaći i posebno definirati od strane dobavljača alata.

3.6. Održavanje i razvijanje sigurnosnih informacijskih politika

Jaka sigurnosna politika određuje karakter cijele organizacije i daje do znanja zaposlenicima što se od njih očekuje. Svi zaposlenici moraju biti svjesni osjetljivosti podataka i svoje odgovornosti za zaštitu tih podataka.

3.6.1. Održavanje politike koja se odnosi na informacijsku sigurnost

Preporučuje se sljedeće:

1. Uspostaviti, objaviti, održavati i distribuirati sigurnosnu politiku koja:
    a. obrađuje sve zahtjeve i preporuke ovog standarda,
    b. uključuje godišnje procedure za identifikaciju sigurnosnih prijetnji i ranjivosti, a rezultat kojih je formalna procjena rizika,
    c. uključuje reviziju barem jednom godišnje kao i osvježavanje politike u skladu s novo unesenim promjenama.
2. Razviti svakodnevne operativne sigurnosne procedure u skladu sa zahtjevima i preporukama ovog standarda (npr. održavanje korisničkih računa, pregledi log zapisa).
3. Razviti procedure korištenja za kritične tehnologije dostupne djelatnicima kao što su modemi i bežična mreža kojima se definira njihovo pravilno korištenje od strane djelatnika i konzultanata. Procedure moraju zahtijevati sljedeće:
    a. eksplicitno odobrenje menadžmenta,
    b. autentikaciju za korištenje tehnologije,
    c. listu svih uređaja i korisnika koji imaju pristup uređajima,
    d. označavanje uređaja s podacima o vlasniku, kontaktnim podacima i svrsi,
    e. dozvoljeni način upotrebe tehnologije,
    f. dozvoljena područja korištenja unutar mreže,
    g. listu proizvoda odobrenih od strane organizacije,
    h. automatsko prekidanje modemske veze nakon određenog perioda neaktivnosti,
    i. aktivaciju modema za dobavljače samo kad je to nužno potrebno, te deaktivaciju odmah nakon završenog korištenja,
    j. onemogućavanje pohranjivanja kartičnih podataka lokalno na tvrdi disk, disketu ili drugi eksterni medij prilikom udaljenog pristupa modemom; onemogućavanje „*cut & paste*“ opcija kao i ispisivanja prilikom udaljenog pristupa.
4. Osigurati da sigurnosna politika jasno definira sigurnosne odgovornosti za sve djelatnike i konzultante.
5. Pridijeliti pojedincima ili timu sljedeće odgovornosti za upravljanje sigurnošću:
    a. uspostavljanje, dokumentiranje i distribuiranje sigurnosnih politika i procedura,
    b. praćenje i analiza sigurnosnih alarma i podataka, te njihova distribucija odgovornim osobama,
    c. uspostavljanje, dokumentiranje i distribucija procedura za reakciju na sigurnosne incidente koje osiguravaju pravovremeno i efektivno djelovanje u takvim situacijama,
    d. administriranje korisničkih računa uključujući kreiranje, brisanje i modifikacije,
    e. kontrola pristupa svim podacima.
6. Pobrinuti se da su svi djelatnici svjesni važnosti sigurnosti kartičnih podataka:
    a. educirati zaposlenike (npr. putem plakata, letaka, memoranduma i promocija),
    b. zahtijevati od zaposlenika pismenu potvrdu o tome kako su razumjeli sigurnosne politike i procedure.
7. Intervjuirati potencijalne nove zaposlenike radi minimiziranja rizika unutarnjih napada.
   Za zaposlenike koji imaju istovremeni pristup samo jednom broju kartice u svrhu obavljanja transakcija, kao što su blagajnici, ovaj zahtjev je samo preporuka.
8. Ugovorom obvezati sve treće strane koje imaju pristup kartičnim podacima da se pridržavaju sigurnosnih pravila kartične industrije. Takav ugovor minimalno mora uključivati:
    a. potvrdu da je treća strana odgovorna za sigurnost kartičnih podataka koje posjeduje,

   b. vlasništvo nad svim zaštićenim imenima vezanim uz kartične podatke i potvrdu da će ta zaštićena imena biti korištena samo u svrhu ostvarenja transakcije ili za drugu svrhu predviđenu zakonom, uz kontrolu od mogućih prevara,
   c. nastavak poslovanja u slučaju velikih incidenata ili katastrofe,
   d. dozvolu da kartična industrija ili od nje ovlaštena treća strana imaju pravo provesti istragu u slučaju sigurnosnog incidenta te potvrdu kako će im biti pružena sva potrebna pomoć; istraga ima svrhu provjere ukoliko se treća strana pridržavala svih standarda kartične industrije za zaštitu kartičnih podataka,
   e. potvrdu da će treća strana i nakon raskida ugovora tretirati kartične podatke kao povjerljive podatke.

9. Implementirati plan za odgovor na sigurnosne incidente. Biti spreman na brz odgovor u slučajevima proboja sustava:
   a. kreirati plan za odgovor na sigurnosni incident pri čemu je potrebno osigurati da plan uključuje minimalno: sigurnosne procedure, procedure za obnavljanje i nastavak poslovanja, procedure za obnovu podataka iz sigurnosnih kopija, uloge i odgovornosti, komunikacijske i kontaktne strategije (npr. za informiranje klijenata i drugih kartičnih organizacija),
   b. testirati plan barem jednom godišnje,
   c. definirati osobe koje će biti dostupne 24 sata dnevno i 7 dana u tjednu u slučaju incidenta,
   d. osigurati prikladno obrazovanje za osobe odgovorne u slučaju incidenata,
   e. uključiti alarme za detekciju i prevenciju upada te sustave za praćenje integriteta podataka,
   f. uspostaviti proces kojim će se moći modificirati plan odgovora na sigurnosni incident prema informacijama dobivenim iz prošlih napada kao i prema razvoju industrijskih standarda.

4. Zaključak

Krađa kartičnih podataka je u današnje vrijeme sve učestalija pojava. *Payment Card Industry Data Security Standard* je odgovor kartične industrije na taj problem kojim se pokušava suzbiti broj tih krađa koje dolaze iznutra, iz same kartične industrije. Standard u biti predstavlja prilično striktno definirane zahtjeve za izradu sigurnosnih politika i procedura. Međutim, područje koje standard ne pokriva i ne može pokriti je upravo područje gdje dolazi do najvećeg broja krađa kartičnih podataka, a to je područje samih korisnika kartica.

Korisnici kartica su najslabija karika u sigurnosnom lancu, a jedino što kartična industrija može učiniti na tom području je edukacija. S druge strane, pod pritiskom konkurencije kartična industrija mora pružiti sve bolje oblike zaštite korisnika od njihovih propusta, pa su tako danas posljedice krađe ili gubitka kartice za korisnika gotove neprimjetne jer ih sve rješava osiguranje kartičnih organizacija. Koliko god to korisniku odgovaralo, to dugoročno predstavlja problem jer bez težih posljedica po korisnika, njegova svjesnost o potrebi zaštite sigurnosti kartičnih podatka neće se promijeniti na bolje.

5. Reference

[1] Payment Card Industry Data Security Standard, MasterCard International, siječanj 2005.

[2] The New Payment Card Industry (PCI) Industry Data Security Standard - Frequently Asked Questions, VigilantMinds Inc., 2005.

[3] Open Web Application Security Project (OWASP), http://www.owasp.org/, rujan 2006.