PCI DSS (Payment Card Industry Data Security Standard)

- Poboljšava bezbednost podataka vlasnika kartica (zaštita podataka na računu)
- Usvajanje bezbednosnih mehanizama i mera na globalnom nivou
- Sensitive data / card holder data
- VISA, MasterCard, JCB, AmericanExpres, Discover – Zajednički standard PCI DSS (2018. najnoviji)
- Ovaj standard je po JDPR-u

12 ZAHTEVA – 6 grupa zahteva

1. BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS (Nije bitno za sam projekat)

- **Install and maintain a firewall configuration to protect cardholder data**
  - Niko ne sme da pristupi kroz neku neautorizovanu adresu
  - Moramo imati mere protiv lažnog predstavljanja
  - Ne smemo prikazivati podatke svima javno na internetu
  - Instalirati firewall na uređaj koji pojedinac ne može da konfiguriše
  - Moramo da imamo review zahteva, moramo da imamo approve, nakon toga neka implementacija
  - S vremena na vreme neki review
  - **MORAMO BITI SVESNI SVIH PROTOKOLA I DNEVNIH PROCEDURA - SVE MORA BITI JASNO**

- **Do not use vendor-supplied defaults for system passwords and other security parameters**
  - **UVEK PROMENITI PODRAZUMEVANE LOZINKE I ONEMOGUĆITI UPOTREBU PODRAZUMEVANIH NALOGA**
  - **Kako testirati? Pokušavati prijavu sa svim default lozinkama**
  - Da li je osoblje svesno da treba promeniti lozinke?
  - **Standardi moraju da budu u skladu sa standardima u industriji – javni, opšte dostupni – JAVNO POZNATE RANJIVOSTI**
  - **PRIRUČNIK SA RANJIVOSTIMA (ako nemamo eksperta) – apdejtovani, nove i stare ranjivosti – SVE KOMPONENTE U SISTEMU**
  - **Brisati nepotrebne funkcionalnosti, skripte itd.**
  - **Sve akcije koje admin ima moraju biti osigurane (šifrovati administrativni pristup)**
  - **BILO KOJI PRISTUP ADMIN INTERFEJSU SE ŠIFRUJE**
  - **Lista softverskih i hardverskih komponenti koja mora biti ažurirana, sadrži ukratko funkcionalnosti, njen status (da li je u opsegu PCI DSS)**
  - **Svi moraju biti upoznati sa propisima, procedurama**

ŠIFRE – Mi biramo kako ćemo da šifrujemo?

- Za simetrične trenutno najsigurniji AES sa 256 bita
- Za asimetrične RSA se lakše implementira – Zašto se smatraju bezbednim? Ne moramo da dajemo drugoj strani svoj ključ
- Kada šifrujemo sa privatnim, a dešifrujemo sa javnim želimo potvrdu identiteta – digitalni potpis
- Heš funkcije – ne postoji lak način da se nađe inverzna funkcija
- U zavisnosti od problema nešto od ovoga ćemo implementirati

2. PROTECT CARDHOLDER DATA (Definitivno mora biti odrađeno u projektu)

- Protect stored cardholder data

- **SVESTI PODATKE KOJI SE SKLADIŠTE NA MINIMUM – ODREDITI POLISU ZADRŽAVANJA PODATAKA**
- **Implementirati neke procedure i procese koji ograničavaju VREME I KOLIČINU podataka**
- **Procesi koji bezbedno brišu podatke koji više nisu u upotrebi**
- **Procesi za zadržavanje podataka sa kartice ako postoji potreba**
- **Na neka tri meseca se identifikuju i brišu podaci koji premašuju limit odnosno vreme zadržavanja**
- **Podaci koji se skladište moraju biti šifrovani ako su definisani kao osetljivi**
- **PODACI ZA AUTENTIFIKACIJU (dokaz ko sam) SE NE ČUVAJU NAKON AUTORIZACIJE (prava pristupa)**
- **npr. kada se unese PIN kod zna se zasigurno ko je vlasnik**
- **ispitamo sve detalje dolazne, odlazne, transakcije, logove, sadržaj baze podataka**
- **CEO PAN BROJ NE SME DA SE PRIKAŽE (Maksimalno prvih 6)**
- **Da li ima smisla da neko može da vidi PAN broj? Bankarski službenik npr.**
- **Iako ja kao korisnik znam PAN broj, NE PRIKAZUJE MI SE ZBOG SIGURNOSTI**
- **Maskiranje PAN broja na stranicama i lista uloga u sistemu koji mogu da vide PAN broj**
- **ONEMOGUĆITI ČITANJE PAN BROJA IZ BAZE (HEŠIRATI PAN BROJ)**
- **Limitirati ko sme da pristupi ključu (najmanji broj mogućih pojedinaca)**
- **DOKUMENTOVATI I PRIMENITI PROCEDURE ZA ZAŠTITU KLJUČEVA**
- **KLJUČEVI ZA ŠIFROVANJE KLJUČEVA TREBA DA BUDU JEDNAKO JAKI KAO I KLJUČEVI ZA ŠIFROVANJE PODATAKA**
- **TREBA DA SE ČUVAJU NA RAZLIČITIM LOKACIJAMA**
- **SMEŠTAJU SE NAJMANJE MOGUĆE LOKACIJA**
- **Ispravno i bezbedno upravljamo ključevima – ČUVAMO I PRENOSIMO BEZBEDNO**
- **Da generišemo jake ključeve, sigurna distribucija, sigurno skladištenje, period trajanja nakon čega treba promeniti ključeve, brisanje i zamena ako postoji potreba za tim, sprečiti neovlašćenu zamenu**
- **Svi moraju biti upoznati sa bezbednosnim politikama – intervju, priča, koriste se svakodnevno**

SERVIS ZA DISTRIBUCIJU KLJUČEVA

- *Man In The Middle* može da presretne i dalje komunikaciju čak iako šaljemo javne ključeve preko tog servisa
- Problem performansi zbog velikog broja ključeva
- Ove probleme možemo donekle da rešimo sa PKI-jem
- **PKI (Public Key Infrastructure) – vezivanje javnih ključeva za identitete subjekata kojima pripada**
- Imao je role, permisije da bi upravljali, distribuirali, skladištili, pozivali, proveravali ključeve
- Radio je sa digitalnim sertifikatima (ko, kome, kada, datum validnosti, javni ključ, digitalni potpis)
- **Mi izdajemo sertifikate za neki domen u kontekstu web sajtova**
- CA izdaje sertifikat – CA potpisuje digitalno taj sertifikat
- **Sertifikati imaju jedinstvene ID-jeve, ako neko podmetne sertifikat ID se razlikuje**
- Sertifikaciona tela nude svoje javne ključeve upotrebom drugih sertifikacionih tela (drugih sertifikata) – tako dolazimo do root-a (Korensko sertifikaciono telo samo sebi potpisuje sertifikat)
- U firmama administratori lokalno instaliraju sertifikate, u web komunikaciji instalirani u browser-u
- Provera validnosti sertifikata
- Razlozi povlačenja sertifikata – datum važenja, došlo je do gubitka ključeva, ako CA nije validan više, neispravna polja
- OCSP tehnika za proveru povučenih sertifikata – serijski broj se prosleđuje I proverava se da li se nalazi na listi povučenih
- **HTTPS – HTTP komunikacija koja se zasniva na transport layer security protokolu**
- **Handshake u sklopu browser-a**
- **SSL preimenovan u TLS – bitno je da se koristi najnovija verzija**

- **Encrypt transmission of cardholder data across open, public networks**
  - **Šifrujemo podatke koje prenosimo preko mreže**
  - **KORISTITI BEZBEDNOSNE PROTOKOLE ZA ZAŠTITU PODATAKA TOKOM PRENOSA – TLS, SSH**
  - **Prihvataju se samo pouzdani sertifikati**
  - **TLS 1 i SSL 2 itd. Imaju javno poznate ranjivosti – KORISTITI SIGURNA VERZIJE PROTOKOLA**
  - **Proveriti da li šaljemo PLAIN PODATKE ili šifrovane podatke (obezbeđene)**
  - **Nezaštićen PAN broj ne sme da se šalje preko EMAIL servisa, CHAT-a i ostalih platformi za razmenu poruka**
  - **PAN broj mora da se kriptuje ako se već koristi neka od ovih tehnologija**

3. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

- **Protect all systems against malware and regularly update anti-virus software or programs (NIJE BITAN ZA PROJEKAT, VEZAN ZA ANTIVIRUS)**
  - Trojanci se lažno predstavljaju
  - Virusi kopiraju sebe i ubacuju se u druge programe, fajlove
  - Crvi se kopiraju po celoj mreži
  - Postaviti antivirus na sve sisteme, redovno održavati, apdejtovati, korisnici ne mogu da ga onemoguće(zabrana interneta, skeniranje sistema) ili izmene, aktivno radi (REAL TIME), nadležno telo daje dozvolu da se antivirus disable-uje
  - Svi su upoznati sa bezbednosnim procesima i procedurama za zaštitu sist3ema od malvera

- **Develop and maintain secure systems and applications**
  - **USPOSTAVITI MEHANIZAM ZA IDENTIFIKACIJU RANJIVOSTI I NJIHOVO RANGIRANJE**
  - **Rangiranje – HIGH, MEDIUM, LOW**
  - **3.2.1 – Prvi broj neka velika izmena, drugi dodavanje novih funkcionalnosti, poslednji broj PATCH je fix bug-ova (MINOR)**
  - **Kada imamo vendor supplied update-ove treba da ih redovno izvršavamo**
  - **Nalozi i šifre se uklanjaju pre developmenta**
  - **Radi se CODE REVIEW**
  - **Razvojno tj. Testno okruženje odvojiti od PRODUKCIJE**
  - **Podela dužnosti**
  - **NE KORISTITI PRAVE PAN BROJEVE PRILIKOM TESTIRANJA**
  - **PISATI SIGURAN KOD, CLEAN CODE, uobičajene smernice za kodiranje**
  - **Kako u kodu uočiti ranjivosti i sortirati ih – trening osoblja**
  - **NEPREKIDNO SE BAVIMO PROCENOM SISTEMA I NJEGOVIM RANJIVOSTIMA**
  - **ISPUNITI STAVKE IZ OWASP TOP 10 LISTE U PROJEKTU**

4. IMPLEMENT STRONG ACCESS CONTROL MEASURES

- **Restrict access to cardholder data by business need to know**
  - **Ograničiti pristup podacima u skladu sa poslovnim potrebama**
  - **Implementirati mehanizam autorizacije**
  - **Treba definisati role i privilegije za svaku rolu**
  - **Minimalan set privilegija**
  - **Treba implementirati na sve komponente**
  - **Ima podešavanja po default-u – Access control**

- ### Identify and authenticate access to system components
  - Svakom pojedincu dodeljujemo ID pre nego što im se omogući pristup sistemu
  - Naloge iz baze brišemo logički
  - Ako nalog nije aktivan duže od 90 dana treba da se obriše
  - Ako imamo 6 neuspešnih pokušaja prijave – nalog se zaključava na određeno vreme
  - Osim ID-a, treba da imamo lozinke i tokene
  - Mehanizam za zaboravljenu lozinku, mehanizam za reset lozinke
  - Ne može da postavi lozinku koju je imao ranije
  - Jaki kredencijali, jaka polisa lozinke (minimum 7 znakova, slova i brojevi, da se menja na 90 dana)
  - Dvostruka potvrda identiteta – kad admin pristupa
  - Dokumentovati procedure za autentifikaciju – smernice kako zaštiti kredencijale, uputstvo za promenu lozinke itd.
  - Svaki pristup bazi treba da bude ograničen – samo admin baze ako takav postoji
  - Sve dokumentovano

5. Regularly monitor and test networks

- ### Track and monitor all access to network resources and cardholder data
  - Mehanizam za praćenje svakog pojedinačnog pristupa (pristupi običnim podacima, pristupi osetljivim podacima razdvojeni), akcije administratora, neuspešna prijava, brisanje
  - Da možemo da izlistamo za svakog korisnika njegove akcije – događaje povezati sa korisnikom
  - Treba da bude automatizovano
  - Sadrži tip događaja, datum i vreme, izvor, ID događaja, poruka
  - Svaki relevantan događaj
  - Sinhronizacija vremena – komponente mogu da imaju neusklađene satove (vremenske zone) – moramo da uskladimo satove
  - Svakodnevno imamo pregled logova koji se tiču operacija nad cardholder data – review logova
  - Čuvati istoriju minimum godinu dana, logovi od poslednja tri meseca treba da budu dostupni online (moraju biti postavljeni online zbog brzog pristupa)
  - Čuvanje osetljivih podataka u logovima – mora biti zaštićeno