Projektiranje sigurnosti

Modeliranje prijetnji
- sigurnosna analiza koja pomaže u otkrivanju najvećih sigurnosnih opasnosti

- cilj je odrediti koje prijetnje i na koji način treba ukloniti
- pretpostavka - proizvod nije siguran ako se ne procijene prijetnje i smanji rizik

Što omogućuje modeliranje prijetnji?

- bolje shvaćanje aplikacije
- pronalaženje pogrešaka
    - procjena da MP pronađe 50% pogrešaka, a ostatak testiranjem i analizom koda
    - pogreške složenih aplikacija, koje se rijetko pronađu drukčije

Načela i proces modeliranja prijetnji

- dugotrajan posao
- bitno je da se obavi kvalitetno
- najbolje iterativno

Proces modeliranja prijetnji

1. Određivanje ciljeva zaštite
2. Arhitektura aplikacije
3. Dekompozicija aplikacije
4. Određivanje prijetnji
5. Dokumentiranje prijetnji
6. Rangiranje prijetnji

Rezultat modeliranja prijetnji =>

- **Dokument s modelima,** definicijom arhitekture i popisom prijetnji

Korak 1 – identifikacija resursa koje treba zaštititi

Korak 2 – Pregled arhitekture

- Dokumentiranje funkcija aplikacije, arhitekture i tehnologija implementacije
- Modeliranje funkcionalnosti (use cases)
- Provjera (kršenja) poslovnih pravila
- Izrađuje se dijagram visoke razine - opisuje strukturu (komponente) sustava

Korak 3 – Dekompozicija aplikacije

- izrada sigurnosnog profila
- Određivanje:
    - granica povjerenja (trust boundaries)
    - toka podataka
    - mjesta unosa
    - privilegiranog koda

Određivanje granica povjerenja

- analiza okruženja resursa određenog dizajnom aplikacije
- za svaki podsustav, procjena je li ulazni tok ili korisnički unos povjerljiv
    - ako nije – razmotriti kako ih autentificirati i autorizirati
- procjena je li pozivajući programski kod povjerljiv
- provjera povjerenja poslužitelja

Određivanje toka podataka

- iterativna dekompozicija
- analizom tokova između podsustava, pa u dubinu

Dijagram toka podatak – notacija

Proces, višestruki proces

- obrada podataka, ili akcija temeljem podataka
- kolekcija potprocesa, može se dekomponirati

Spremište podataka

- Bilo koji oblik pohrane (datoteka, BP, …)

Granica povjerenja

- oznaka promjene privilegije (razine prava nad podacima)

Vanjski entitet, sudionik

- sve što je izvan aplikacije, a u interakciji putem točke unosa

Tok podataka

- usmjereno kretanje podatka unutar aplikacije

Ostale aktivnosti dekompozicije

- Određivanje točki unosa
- Određivanje privilegiranog koda
- Dokumentiranje profila sigurnosti

Korak 4 - Određivanje prijetnji

- Odrađuju razvojni tim i tim za testiranje

Osnovni pristupi:

1. **STRIDE****

- **S**poofing – zavaravanje, lažiranje
- **T**ampering [with Data] – zlonamjerna izmjena podataka
- **R**epudiation – nepriznavanje, poricanje
- **I**nformation disclosure - otkrivanje informacija
- **D**enial of service - uskraćivanje usluge
- **E**levation of privilege - povišenje ovlasti

postupak:

Provodi se tako da se sustav raščlanjuje u relevantne komponente pa se onda:

- procjenjuje osjetljivost na prijetnje svake komponente (analiza dijagramom toka podataka)
- prijetnje se smanjuju (mitigation) prikladnim svojstvima sigurnosti
- ponavlja se (rekurzivno) do zadovoljavajućeg rezultata

2. **Kategorizirane liste prijetnji** - popis uobičajeno "sumnjivih" prijetnji
3. **Stabla prijetnji**
   Za svaku komponentu dobivenu dekompozicijom
   - određuju se moguće prijetnje
   - utvrđuje se način na koji se prijetnje odražavaju na sustav
   - Primjer
     - korijen predstavlja prijetnju
     - djeca predstavljaju korake koje napadač mora poduzeti da bi ostvario prijetnju
4. **Obrasci napada**
   Općenita reprezentacija uobičajenih napada
   - definira cilj, uvjete, tehniku i rezultat napada
   - Naglasak je na **tehnici napada** (kod **STRIDE** na **ciljevima napadača**)

Korak 5 - Dokumentiranje prijetnji
Predložak za evidenciju prijetnji

- svakako se popunjavaju opis i cilj
- rizik se ostavlja za naredni korak
- ostali atributi mogu biti opcionalni (tehnike napada, protumjere)

Korak 6 - Rangiranje prijetnji
često se koriste tehnike za određivanje rizika

- **rizik** = **vjerojatnost događaja * potencijalna šteta**
- **vjerojatnost** npr. u rasponu 1-10
- **šteta** npr. u rasponu 1-10
- **rizik** u rasponu 1-100
- raspodjela u tri grupe (**visok**, **srednji**, **nizak**) koje predstavljaju prioritete

DREAD (model procjene rizika)**

DREAD – klasifikacija računalnih prijetnji

- **Damage potential** – moguća šteta, veličina štete bude li napad uspješan
- **Reproducibility** – reproduktivnost, koliko je jednostavno ponoviti napad
- **Exploitability** – iskoristivost, trud i znanje potrebnih za uspješan napad
- **Affected users** – zahvaćeni korisnici, moguće uspjelim napadom, postotno
- **Discoverability** – mogućnost otkrivanja, teško mjerljivo

Procjena svake prijetnje po navedenim parametrima

- pojedinačno vrijednost od 1 do 10 (najmanje loše – najgore)
- **ukupan rizik** - prosjek 5 pojedinačnih **DREAD** vrijednosti

Bolje – (jednostavna) shema ocjenjivanja

- Nisko, srednje, visoko – preslikano u interval 1 do 3
- Zbrajaju se vrijednosti (1-3) za zadanu prijetnju
    - rezultat je u rasponu 5-15
- pridjeljuje se rizik, npr. 5-7 nizak, 8-11 srednji, 12-15 visok

Razrješenje prijetnji (nakon modeliranja)

- Popraviti (smanjenje, redukcija rizika)
- Ne učiniti ništa (prihvatiti rizik)
- Obavijestiti korisnika te mu prepustiti odluku o korištenju (prijenos)
- Uklanjanje rizičnog svojstva (izbjegavanje)

Smanjenje površine napada

Površina napada - kolekcija ulaznih točaka programskog proizvoda

- mjera "napadljivosti"
- Veća površina napada = više posla zaštite = veća potencijalna šteta
- Površina određuje rizik napada – mjera potencijalnog pristupa i udara

Združeni model površine napada

- kontrole pristupa smanjuju
    - mogućnost da se dosegne sustav
    - broj elemenata koji su vidljivi ili se mogu koristiti

Smanjenje površine napada

Glavni ciljevi

- Smanjenje količine koda koji se izvodi „po viđenju” (by default)
- Smanjenje količine koda kojem mogu pristupiti nepouzdani (untrusted) korisnici, „po viđenju”
- Zatvaranje pristupnih točaka (access points, entry points) – vrata koja se lako otvaraju/iskorištavaju
- Ograničavanje štete u slučaju da pristupna točka bude iskorištena

Krajnji cilj – odbijanje budućih napada

Uobičajena metrika softverske sigurnosti

- Razina programskog koda - brojanje bugova
- Razina proizvoda/sustava
    - Brojanje koliko puta je verzija sustava spomenuta u CERT, MITRE CVE, … biltenima

Mjerenje površine napada

- Mjerenje „avenija” napada
    - Možebitno napadane mogućnosti
- Mjerenje relativne sigurnosti
    - Delta mjerenje – razlike između verzija istog proizvoda
- Postupak
    - Osnovica (baseline) + tjedna mjerenja
    - Određivanje minimalne površine na početku
    - Ako se površina povećava – odrediti kako ju smanjiti

Proces ASR (attack surface reduction)

- Ustanovljavanje pristupnih točki
- Rangiranje točaka - prema korisniku
- Podešavanje

Najbolje prakse

Redukcija koda koji se izvodi *by default*

- Isključiti mogućnost koju ne koristi barem 80% korisnika
- Zaustavljen servis ne može biti napadnut
- Smanjenje pristupa od strane nepouzdanih (untrusted) korisnika
    - Ograničenje pristupa na lokalnu mrežu ili raspon IP adresa
    - Autentifikacija
- Redukcija privilegija radi ograničavanja potencijalne štete
- Definiranje površine napada tijekom dizajna/projektiranja

Provjera sigurnosti

Provjera ispravnosti softvera (općenito)

- Testiranje programa, provjeravanje programa, ispitivanje programa
- Prema svrsi testiranja – verifikacija i validacija
- Prema objektu provjere – strukturalno i funkcionalno
- Prema načinu provjere – statička analiza i dinamička analiza

Ključni pojmovi

- **[„normalan”] Test** - provjerava je li neki aspekt softvera ispravan
- **Test sigurnosti** - nastoji dokazati da neki dio ne radi kako treba
- **Pogreška (error)** - propust programera, npr. radi nerazumijevanja
- **Kvar (fault), defekt (defect), neformalno bug** - neispravan dio koda
- **Zastoj u radu (failure)** - stanje izazvano jednim ili više kvarova
- **Ispravak (Fix)** - stanje popravka

Postupci provjere sigurnosti aplikacija

- Nadzor
- Static Application Security Testing (**SAST**)
- Dynamic Application Security Testing (**DAST**)
- Interactive Application Security Testing (**IAST**)
- Analiza izvornog koda - statička ili dinamička s pristupom čitavom kodu

1. Nadzor

Varijante

- Inspekcija (inspection)
- Timski pregled (team review)
- Prohod (walkthrough)

Nadzor omogućuje:

- nalaženje defekata ranije u životnom ciklusu - do 80% prije testiranja
- nalaženje defekata s manje napora nego testiranjem
- nalaženje drugačijih defekata nego testiranjem - problemi dizajna i zahtjeva

1. **Inspekcija****
    - Formalni proces
    - Temeljita pokrivenost odvojenim ulogama
        - **Moderator** - vodi sastanak, prati probleme
        - **Čitalac** - parafrazira (prepričava) kod, nije autor
        - **Zapisničar** - evidentira defekte
        - **Autor** - osigurava kontekst koda, objašnjava, popravlja nakon pregleda
    - **Aktivnosti**:
        - Izrada kontrolnih listi za specifične ciljeve
        - Prikupljanje podataka za praćenje pogrešaka
        - Određivanje potrebe za narednim inspekcijama
    - Opsežna dokumentacija učinkovitosti
    - ***Proces inspekcije***
    - **Planiranje**
        - autor inicira, moderator ekipira, skupa pripreme inspekcijski paket
    - **Priprema**
        - recenzenti pregledavaju, koriste kontrolne liste i analitičke alate, označavaju defekte
    - **Sastanak**
        - čitalac prepričava, recenzenti komentiraju i zapitkuju, zapisničar evidentira
        - tim zaključuje procjenu koda
    - **Prerada** - autor popravlja
    - **Kontrola** (follow-up)
        - moderator verificira korektnost promjena, autor prijavljuje kod (check-in)

2. **Timski pregled**
   - Timski pregled ("lagana" inspekcija)
   - Osobe: moderator, recenzenti (koji nisu autori koda)
   - Moduli ili manji skupovi klasa
   - 1-2 sata, < 1 kLOC

3. **Prohod (walkthrough)**
   - Autor vodi sastanak i objašnjava kod
   - Manje formalan proces
   - Nedefiniran proces
   - Nema kontrolnih lista ili metrike

Ostali postupci: *programiranje u paru, peer deskcheck, pass around*

Statička provjera**

- **SAST (Quick and Dirty)**
  - Analiza koda bez izvršavanja
  - Obuhvaća sve osim testiranja
  - Korištenje analizatora koda
  - Može biti dio revizije koda
- Ograničenja: pogrešno otkrivanje (**false postive**) i pogrešno neprepoznavanje (**false negative**)
- **Vrste statičke analize**
  - Provjera tipova
  - Provjera stila
  - Razumijevanje programa – zaključivanje značenja
  - Provjera svojstava - osiguranje da nema lošeg ponašanja
  - Verifikacija programa - osiguranje ispravnog ponašanja
  - Traženje pogrešaka
- **Mehanizmi statičke analize**
  - Parser
  - Model Builder
  - Analysis Engine
- **Tehnike analize**
  - Leksička analiza i parsiranje
  - Analiza toka podataka
  - Analiza „mrlja" - identifikacija varijabli uprljanih korisničkim unosom
  - Pravila propagacije mrlja : pravila izvora, pravila slivnika, pravila propuštanja, pravila čišćenja, pravila početka
- **Prednosti statičke analize**
  - Potpuna pokrivenost koda (code coverage) - u teoriji
  - Potencijal potvrde izostanka čitavih klasa bugova
  - Hvata bugove različite u odnosu na dinamičku analizu

- **Slabosti statičke analize**
    - Visok postotak pogrešnog otkrivanja
    - Teško oblikovanje testa
    - Složenost izgradnje (alata) - „parser za svaki jezik"
    - Neimanje cjelokupnog izvornog koda u praksi
- **Alati za statičku analizu – StyleCop, CodeSmart**

Dinamička provjera**

Fuzzing - "pročešljavanje"

- ubrizgavanje kvara u aplikaciju (fuzzing, fuzz testing)
- slanje neispravnih, neočekivanih ili nasumičnih podataka ulazu programa
- slično regresiji, samo s lošim podacima
- „češljanje" aplikacija, protokola, datoteka
- **PREDNOSTI**: jednostavnost, nezavisnost o platformi, jeziku
- **NEDOSTACI**:
    - primjena na uzak skup povredivosti
    - složena primjena na tehnologije
    - relativno dugo trajanje
- **Postupci:**
    - Glupo = Dumb (mutational) fuzzing
        - dovoljno manje znanja o cilju i alatima
        - pseudoslučajne anomalije ispravnih podataka
    - Pametno = Smart (generational) fuzzing
        - podaci generirani na temelju modela
        - zahtijeva dubinsko poznavanje cilja i specijaliziranih alata
        - Smišljene anomalije poznavanjem formata, standarda
- Alati: **CERT BFF** i **FOE**

Penetracijsko testiranje (Pen Test), etičko hakiranje

- procjena sigurnosti sustava ili mreže simuliranjem zlonamjernog napada
- osoba, ekipa, poželjno vanjski konzultanti (?)
- pismena dozvola vlasnika (provedbe nezakonitih aktivnosti)

Svrha

- Potvrda funkcionalnosti sigurnosnih kontrola
- Pravovremeno uočavanje sigurnosnih propusta
- Prevencija sigurnosnih incidenata
- Opravdavanje investicije
- Ispunjavanje regulatornih zahtjeva

Pristup penetracijskom testiranju

- bez dostupnih informacija
- sa svim informacijama
- s djelomično dostupnim informacijama

Kriterij početne točke testa

- Vanjski - s udaljene lokacije
- Unutrašnji - s intraneta

Ostali kriteriji - opseg, prikrivenost, tehnike, agresivnost
Izvođenje penetracijskog testa

Istraživanje (eng. reconnaissance), izviđanje

- ispitivač pokušava prikupiti što više informacija.
- **pasivno** - javno dostupne informacije (npr. podaci s društvenih mreža, Google)
- **aktivno** - istraživački alati (npr. nslookup), da bi se odredili određeni parametri

Skeniranje (eng. scanning)

- ispitivač skenira otvorene portove (port scanning) korištenjem alata (npr. Nmap)
- cilj - enumeracija servisa, verzije enumeriranih servisa i OS (OS and service fingerprinting).
- skeniranje ranjivosti (vulnerability scanning), automatiziranim alatima (npr. OpenVAS)

Dobivanje pristupa (eng. obtaining access)

- iskorištavanje ranjivosti, ručno ili alatom (npr. Metasploit),
- ovisno o dogovoru s vlasnikom, neke ranjivosti se neće iskorištavati (npr. rušenje poslužitelja)

Zadržavanje pristupa (eng. maintaining access)

- ispitivač instalira zloćudne backdoor i rootkit programe za daljnji pristup sustavu
- ova i naredna faza se u praksi najčešće ne provode ali predstavljaju scenarij realnog napada

Brisanje tragova (eng. erasing evidence)

- ispitivač pokušava izbrisati dnevničke zapise koji bi ukazivali na njihov neovlašteni pristup

Alati za penetracijsko testiranje i detekciju upada

- Brutus (lozinke), Snort

Upravljanje (softverskim) rizikom

Rizik

- uvjet koji može dovesti do nekih gubitaka ili može ugroziti uspješnost projekta

Upravljanje rizikom

- suočavanje s brigom prije nego što ona preraste u problem ili krizu
- **sastavnice**:
  - identifikacija rizika
  - odluke kako postupiti u slučaju pojedinog rizika
  - uklanjanje rizika i rukovanje posljedicom rizika

Aktivnosti upravljanja trebaju odgovarati veličini projekta

- **Mali** projekti - jednostavne liste rizika, jedan član ekipe (ne voditelj)
- **Veliki** projekti - formalno upravljanje rizikom, risk officer, puno radno vrijeme

Procjena rizika

Identifikacija rizika

Opis rizika izjavama oblika uzrok-posljedica

- Prati se zabrinjavajuće stanje i procjenjuje moguća posljedica
- Jedan uvjet može dovesti do nekoliko posljedica, a nekoliko uvjeta može doprinijeti istoj posljedici

Rizici rokova

Rizici planiranja

Rizici organizacije i upravljanja

Rizici razvojnog okruženja

Rizici krajnjeg korisnika

Rizici naručitelja

Rizici (pod)ugovaratelja

Rizici zahtjeva

Rizici aplikacije

Rizici vanjskih utjecaja

Rizici razvojne ekipe

Rizici dizajna i ugradnje

Rizici procesa

Analiza rizika

Nakon utvrđivanja liste rizika projekta

- Analiza svakog rizika pojedinačno
- Utvrđivanje utjecaja na projekt

Primjena

- odabir između nekoliko razvojnih opcija ili utvrđivanje rizika već odabrane razvojne opcije

Dokumentiranje rizika

Predložak za dokumentiranje pojedine izjave o riziku

- **ID**: Jedinstveni identifikator
- **Datum otvaranja**: Datum kada je rizik identificiran
- **Datum zatvaranja**: Datum kada je rizik zatvoren
- **Opis**: Opis rizika u obliku «uvjet-posljedica»
- **Vjerojatnost**: Vjerojatnost da će rizik postati problem
- **Učinak**: Potencijalna šteta ako se problem ostvari
- **Izloženost**: Vjerojatnost * učinak
- **Plan razrješenja**: izbjegavanje, smanjenje, transfer, prihvaćanje rizika
- **Nositelj**: Osoba odgovorna za razrješenje rizika
- **Rok**: Datum do kojeg plan ublaživanja mora biti završen

Vrednovanje rizika

- Vjerojatnost gubitka se kreće u rasponu od 0.01 do 1.0 (do 100%)
- Veličina gubitka, učinak
    - zanima nas vremenski raspored
    - alternativno financijski gubitak u novčanim jedinicama
- Izloženost, utjecaj
    - Izloženost = Vjerojatnost * Učinak
- Ponekad nije potrebno precizno kvantificirati rizik (visoko, srednje, nisko)

Procjena veličine gubitka

Kada nije jednostavno izravno procijeniti veličinu gubitka, moguće gubitke podijeliti u manje, te procijeniti njihovu veličinu, a zatim zbrojiti pojedinačne procjene podgubitaka

---

Procjena vjerojatnosti gubitka

Najupućenija osoba procijeni vjerojatnost svakog pojedinačnog gubitka

Delphi ili neki drugi postupak kojim se postiže konsenzus

- Svaki član grupe zasebno procjenjuje svaki rizik
- Diskutiraju se (argumentiraju) procjene, naročito ekstremne
- Postupak procjene se ponavlja do konvergencije

Metoda klađenja

Npr. "Ako dodaci budu gotovi na vrijeme dajem/dobivate 125kn, inače ja dobivam 100kn"

- Oklada se prepravlja sve dok obje strane ne budu zadovoljne
- Vjerojatnost rizika je rezultat dijeljenja dobitka ponuditelja oklade i ukupnog iznosa.
- Za navedeni primjer, vjerojatnost = 100 kn / (100 + 125) kn = 44%.

Vremenski gubici cijelog projekta i vremenske zalihe

Izloženost riziku je očekivana **vrijednost vremenskih gubitaka**

- Statistički, očekivani gubitak je umnožak vjerojatnosti i veličine gubitka

Ukupni gubici prije poduzimanja koraka za upravljanje rizikom

Vremenski plan treba **prilagoditi** očekivanim vremenskim gubicima

- nakon izrade plana upravljanja rizikom
- postaviti očekivane **vremenske gubitke** kao **vremensku rezervu projekta**

Utvrđivanje prioriteta rizika

- Postavljanje prioriteta rizika – usmjeravanje upravljanja
- Jednostavnije je usredotočiti se samo na vremenske rizike, nego na sve vrste rizika odjednom!

Točnost procjene i zanemarivanje rizika

- Poredak rizika prema prioritetu je samo aproksimacija
- Točnost prioriteta zavisi o točnosti procjena vjerojatnosti i veličina
- **Zanemarivanje rizika**
    - Nema smisla trošiti vrijeme na rizike koji nose male gubitke

---

Kontrola rizika

1. Planiranje upravljanja rizikom
2. Razrješenje rizika
3. Nadziranje, praćenje rizika

Plan upravljanja rizikom

- Radi se plan djelovanja za svaki utvrđeni visoki rizik
- Plan može biti samo izjava „tko, što, gdje, kada, zašto i kako” postupiti
- Plan treba sadržavati opće odredbe za nadzor rizika, zatvaranje rizika koji su riješeni i identifikaciju novih rizika

Razrješenje rizika - ovisi o posebnostima pojedinog rizika

- **Izbjegavanje rizika** - ne preuzeti rizik ili ukloniti uzrok
- **Preusmjeravanje rizika** - rizik u jednom dijelu nije rizik u nekom drugom
    - posljedice i/ili upravljanje prenesu se u drugi dio projekta ili na treću stranu
- **Smanjenje rizika -** Prihvatiti mogućnost rizika i razviti rezervni plan
- **Prihvaćanje rizika -** Prihvatiti mogućnost da se rizik može dogoditi i ne činiti ništa
- ostalo:
    - Prikupljanje informacija o riziku
    - Objavljivanje rizika
    - Evidencija rizika

Nadgledanje rizika

- rizici se pojavljuju, povećavaju/smanjuju, nestaju s vremenom
- trajno nadgledanje i mjerenje

„lista najvećih 10" (Top 10)

- jedna od najboljih strategija za nadgledanje
- **sadržaj** - status rizika, broj pojavljivanja, koraci od prethodnog ažuriranja
- **ažuriranje jednom tjedno** (ili prema iteraciji životnog ciklusa projekta)
- **najvažniji aspekt** - osiguranje redovitog uvida, redovno razmišljanje o rizicima uzbunjivanje u slučaju promjena u važnosti rizika

Kvalitativna procjena rizika

numerički, ali relativnim vrijednostima

Matrica preddefiniranih vrijednosti

- razina rizika kao suma vrijednosti sredstva (AV), ranjivosti (V) i prijetnje (T), pr.
- AV u rasponu od 0 (mala) do 4 (vrlo velika)
- V i T raspon od 0 (niska razina) do 2 (visoka razina)
- R = AV +V +T

Vrijednosti 0-8

- Nisko (M): 0 - 2
- Srednje (S): 3 - 5
- Visoko (V): 6 – 8

Planiranje kontinuiteta poslovanja za nepredviđene slučajeve

Štetni događaj (adverse event)

- Događaj s negativnim posljedicama koji bi mogao ugroziti resurse ili operacije organizacije – napad, sabotaža, potres, poplava, požar, curenje plina, radijacija
- Mogući kandidat za incident

Incident

- Štetni događaj koji može rezultirati gubitkom informacijske imovine, ali trenutno ne prijeti održivosti čitave organizacije
- Jasno identificirani napad na informacijsku imovinu koji može ugroziti njenu povjerljivost, cjelovitost ili raspoloživost

Katastrofa (disaster)

- Štetni događaj koji bi mogao ugroziti održivost čitave organizacije
- Eskalira iz incidenta ili odmah bude proglašena

Planiranje za nepredviđene situacije (Contingency planning - CP)

- više rukovodstvo odredi što kada štetni događaj postane incident ili katastrofa

Elementi

- Analiza utjecaja na poslovanje (Business Impact Analysis - BIA)
- Planiranje odgovora na incidente (IR), oporavka od katastrofe (DR) i kontinuiteta poslovanja

Planovi

- Plan za nepredviđene situacije
- Plan za odgovora na incident
- Plan oporavka od katastrofe
- Plan kontinuiteta poslovanja
- Dodatno, upravljanje krizom

Tim za upravljanje planiranjem nepredviđenih situacija

- Grupa viših menadžera i članova projekta organizirani da pro/vode sve napore CP
- Formiranje tima i dodjela uloga prije nego započne planiranje

Prvak, **šampion** (champion) - Viši rukovoditelj – potpora, promicanje, podržavanje (CIO/CEO)

Voditelj projekta (project manager) - Srednji rukovoditelj ili CISO

Članovi tima - Rukovoditelji ili predstavnici: poslovanje, IT, informacijska sigurnost

Cjelokupni proces planiranja za nepredviđene situacije

- Razvoj politike CP
- Provedba BIA
- Određivanje preventivnih kontrola
- Izrada strategija za nepredviđene situacije
- Razvoj plana za nepredviđene situacije
- Osiguranje plana provjere, treninga i uvježbavanja
- Osiguranje održavanja plana

Glavni koraci planiranja za nepredviđene situacije

- Formiranje tima za krizno planiranje (CPMT)
- Razvoj izjave o politici CP
- Provedba analize utjecaja na poslovanje
- Formiranje podređenih timova
- Razvoj podređenih politika
- Integracija analize utjecaja na poslovanje (BIA)
- Utvrđivanje preventivnih kontrola
- Organiziranje timova za odgovor
- Razvoj strategija odgovora (contingency strategies)
- Razvoj podređenih planova
- Testiranje plana, trening i vježbe
- Održavanje plana

Analiza utjecaja na poslovanje (Business Impact Analysis - BIA)

Nastoji odgovoriti na sljedeće:

- **Doseg**: koje organizacijske cjeline i sustave obuhvatiti
- **Plan**: podaci mogu biti obimni – uvažiti relevantne
- **Ravnoteža**: objektivno-subjektivno, naglasak na znanju i iskustvu osoblja
- **Cilj**: odrediti ključne donositelje odluka – informacije za donošenje
- **Praćenje**: povremena provjera da vlasnici procesa i donositelji odluka podržavaju proces i rezultat BIA

Koraci BIA

NIST SP 800-34 (National Institute of Standards and Technology)

- Identifikacija ključnih poslovnih procesa i funkcija,
- Utvrđivanje međuovisnosti informacijskih sustava i poslovnih procesa,
- Utvrđivanje prioriteta i klasifikacija poslovnih procesa i funkcija,
- Utvrđivanje utjecaja prekida poslovnih procesa na sveukupne poslovne operacije, s naglaskom na financijske i operativne utjecaje,
- Utvrđivanje zahtijevanih vremena oporavka,
- Utvrđivanje preduvjeta za oporavak poslovanja,
- Utvrđivanje redoslijeda oporavka pojedinih procesa i funkcija

Identifikacija poslovnih procesa i funkcija te procjena utjecaja

- **Kritične funkcije (critical functions)** - neophodne za poslovanje
  - IT gledište - prekid ima ozbiljne/trajne sigurnosne, operativne i financijske učinke
  - Prihvatljivo vrijeme oporavka mjeri se satima
- Bitne funkcije (essential functions) - vrlo važne, ali ne ključne
  - Pr. isplata plaće zaposlenicima
  - Prihvatljivo vrijeme oporavka u IT segmentu – dan ili dva
- Potrebne funkcije (necessary functions)
  - Pr. E-pošta ili pristup Internetu, funkcije potpore poslovnim procesima
  - Prihvatljivo vrijeme oporavka mjeri se danima
- Poželjne funkcije (desirable functions) - mali učinak na poslovanje
  - Prihvatljivo vrijeme oporavka – tjednima ili mjesecima

Zahtjevi oporavka

Ciljana točka oporavka – RPO

- Vremenska tolerancija gubitka podataka, stanje povrata oporavkom pričuvne kopije podataka
- Vrijeme između posljednjeg backupa i prekidnog događaja

Ciljano vrijeme oporavka - RTO (Recovery Time Objective)

- Maksimalno vrijeme za oporavak resursa koji podržavaju misiju organizacije
- Vrijeme između prekidnog događaja i oporavka sustava/resursa

Vrijeme oporavka rada - WRT (Work Recovery Time)

- Vrijeme potpunog oporavka poslovne funkcije nakon oporavka resursa
- Obnova podataka (elektronički restore i ručni unos) + testiranje i validacija

Maksimalno prihvatljivo vrijeme ispada – MTD

- Maksimalno podnošljiv zastoj/ispad sustava mjeren trajanjem neraspoloživosti poslovnih procesa
- Period između prekidnog događaja i početka normalnog poslovanja

MTD = RTO + WRT

Izvješće o analizi utjecaja

- Ključni procesi i funkcije,
- Međuovisnosti procesa i IT resursa,
- Kritičnost odnosno razina utjecaja na poslovanje,
- Ključne uloge i odgovornosti osoba zaduženih za njihovu provedbu,
  Zahtijevana vremena oporavka,
- Financijski, operativni, pravni, personalni učinci nedostupnosti,
- Ručne procedure za nastavak poslovanja u slučaju nedostupnosti

Planiranje odgovora na incidente (IRP)

- Tim za planiranje odgovora na incident
- Tim za odgovor na incident
- **Faze odgovora na incident**
    - Planiranje (planning)
    - Detekcija (detection)
    - Reakcija (reaction)
    - Oporavak (recovery)

Politika odgovora na incidente

NIST 800-61, Rev. 2, The Computer Security Incident Handling Guide

Izjava o svrsi i ciljevima politike

- Doseg – na koga se što odnosi te u kojim okolnostima
- Definicija incidenata i povezanih pojmova
- Organizacijska struktura, definicija uloga, odgovornosti i ovlasti
- Postavljanje prioriteta ili ocjene ozbiljnosti incidenata
- Mjerenje učinaka (kontrola pristupa, sigurnosne stijene, DNS, …)
- Izvještavanje i formulari

Detekcija incidenta

Indikatori mogućih incidenata

- Nepoznate datoteke
- Nepoznati procesi
- Neuobičajeno trošenje računalnih resursa
- Neuobičajen pad sustava

Indikatori vjerojatnih incidenata

- Aktivnosti u neuobičajena vremena (mrežni promet ili pristup datotekama „kada ih nitko ne koristi“)
- Pojava novih vjerodajnica
- Napadi prijavljeni od strane korisnika
- Notifikacije IDPS (Intrusion Detection / Prevention System)

Indikatori izvjesnih incidenata

- Korištenje neaktivnih vjerodajnica
- Izmjene dnevničkih zapisa (u odnosu na rezervnu kopiju)
- Prisustvo hakerskih alata
- Dojava partnera ili parnjaka (partner, peer)
- Poruka hakera – „gotcha“ na web stranici ili email poruka sa „sigurnog“ računa

Reakcija – ključni pojmovi
Poruka upozorenja (alert message)

- Opis incidenta s dovoljno informacija
- Da svaka osoba zna koji dio IR plana provesti bez da uspori obavješćivanje

Popis upozorenja (alert roster)

- Kontakti koje treba obavijestiti o događaju incidenta
- Hijerarhijski popis (hierarchical roster)
    - Popis upozorenja u kojem prva osoba poziva nekoliko drugih, a one dalje
- Slijedni popis (sequential roster)
    - Popis upozorenja u kojem jedna osoba poziva svaku na popisu

Reakcija – postupak

1. Obavještavanje *pravih* ljudi
2. Dokumentiranje incidenta
    a. Tko, što, kada, gdje, zašto i kako
    b. Studijski slučaj, učenje
    c. Dokaz za ispravno postupanje
    d. Podloga za simulacije u budućnosti
3. Strategije suzbijanja incidenata i povrata kontrole

Oporavak od incidenta

Ulaganje napora po prioritetima – slijeđenjem plana

Procjena štete

- trenutno, danima, tjednima
- Procjena sustava i pohrane podataka
- Proučavanje dnevnika (log), računalna forenzika, prikupljanje dokaza

Oporavak

- Identifikacija ranjivosti
- Instalacija, zamjena, nadogradnja zaštite
- Oporavak podataka, usluga, procesa
- Kontinuirano praćenje/nadzor sustava
- Obnavljanje povjerenja

Naknadna revizija

Oporavak od katastrofe

- neželjeni i neočekivani štetni događaj koji organizaciji
- onemogućuje obavljanje kritičnih poslovnih funkcija
- kroz neodređeni vremenski period i
- rezultira velikom štetom (ne samo financijskom) za njezino poslovanje

Primjeri katastrofa:

- nedostupnost glavne lokacije organizacije zbog prirodne katastrofe ili požara,
- nedostupnost IT infrastrukture na glavnoj lokaciji zbog kvara hardvera ili softvera većih razmjera,
- nedostupnost ključnih djelatnika organizacije zbog epidemije,
- dugotrajni prekid isporuke električne energije,
- prekid ključnih usluga dobavljača

Sadržaj plana oporavka od katastrofe (DR plan)

- Popis IT sredstava
    - inventura hardvera, sustava i aplikacija
- Procjena rizika
    - za svaki ključni IS; vjerojatnost, posljedice
- Klasifikacija važnosti
- RPO i RTO
- Popis aktivnosti – procedure uspostave nastavka poslovanja

Aktivnosti oporavka

- **Oporavak hardvera**
    - Zamjena komponenti na glavnoj ili pričuvnoj lokaciji
    - Poslužitelji, mrežna oprema, vatrozid, IP/DS
- **Oporavak operacijskih sustava**
    - OS i glavni servisi (npr. DNS, AD)
- **Oporavak baza podataka i arhivskih zapisa**
- **Oporavak spremišta podataka**
    - Storage, pričuvni hardver (Storage Area Network – SAN)
- **Oporavak aplikacija**
    - Podaci, sinkronizacija s pričuvnom lokacijom, provjera
- **Testiranje procedura oporavka**

Razine oporavka od katastrofe

Razina 0 – bez pohrane podataka na pričuvnoj lokaciji

- Oporavak je moguć samo korištenjem sustava na primarnoj lokaciji

Razina 1 – Izrada pričuvne kopije podataka s hladnom lokacijom

- Podatci se pohranjuju na diskove/trake i fizički šalju na pričuvnu hladnu lokaciju
- Jeftino rješenje, nastavak rada obično moguć tek nakon nekoliko dana

Razina 2 – Izrada pričuvne kopije podataka s vrućom lokacijom

- Pričuvne kopije se fizički šalju na pričuvnu lokaciju - PTAM
- Pričuvna **vruća** lokacija

Razina 3 – Elektronička pohrana

- BC2 + Kritični podaci elektronički na pričuvnu lokaciju

Razina 4 – Aktivna pričuvna lokacija

- Svi podatci periodički elektronički kopirani na pričuvnu lokaciju

Razina 5 – Integritet transakcija

- Aplikacijski podatci i podatci iz BP se na transakcijskoj razini preslikavaju na diskove na pričuvnoj lokaciji

Razina 6 – Minimalni ili nikakav gubitak podataka

- Svi podatci (neovisno o aplikaciji) se „trenutno" kopiraju s primarne na pričuvnu
- Elektronički najčešće zrcaljenjem diska

Razina 7 – Potpuno automatizirano rješenje

- Nadgradnja razine 6 pri kojoj u slučaju katastrofe IS automatski nastavlja raditi na hardverskoj infrastrukturi, aplikacijama i podatcima koji se nalaze na pričuvnoj lokaciji bez ikakvog prekida ili gubitka podataka

Varijante pričuvne lokacije

- **Cold** – infrastruktura
- **Warm** – bez aplikacija
- **Hot** – potpuna konfiguracija

Procedure za prelazak s primarne na pričuvnu lokaciju i obrnuto

Failover (activation)

- Automatski nastavak rada na pričuvnom poslužitelju, računalnoj ili mrežnoj komponenti u slučaju kvara na primarnom P/RK/MK
- Pravi automatizirani failover moguć samo na razini BC7

Switchover (role switch)

- Kontrolirana zamjena uloga, najčešće ručno u planirano vrijeme
- Priprema za održavanje – instalacija zakrpa, nadogradnji, …
- Također za prelazak na pričuvnu kada je failover prekompliciran ili preskup

Failback

- Nakon osposobljavanja sustava na primarnoj lokaciji
- Vraćanje promjena u podacima i aplikacijama
- U idealnom slučaju (BC7) automatski
- U praksi uz manji ili veći gubitak podataka, ovisno o rješenju

Planiranje kontinuiteta poslovanja

- Napori organizacije da nastavi s kritičnim funkcijama u slučaju ispada primarne lokacije
- Uspostava sustava upravljanja kontinuitetom poslovanja prema normi:
  - ISO 22301
  - ISO 22313

Proces slijedi četiri ključna načela: **Fokus, Preventiva, Plan, Zaštita**

- Upravljanje rizikom
- Analiza posljedica na poslovanje (BIA)
- Razvoj strategije kontinuiranog poslovanja
- Razvoj BC plana
- Testiranje BC plana
- Održavanje BC plana

Izvođenje plana BC

1. Početni odgovor i obavijest
2. Procjena problema i eskalacija
3. Izjava o katastrofi / prekidnom događaju
4. Implementacija plana logistike
5. Oporavak i nastavak poslovanja
6. Normalizacija

Uloge i odgovornosti pri izvođenju plana BC

- ERT – Emergency Response Team
- CMT – Crisis Management Team
- DAT – Data Team
- NT – Notification Team
- CCT – Command & Control Team
- RPLT – Resource Procurement and Logistics Team
- UMT – User Management Team
- BUT – Business Unit Team

Sigurnost u sustavima za elektroničko poslovanje

Suvremeni **elektronički dokumenti** koji se razmjenjuju u elektroničkom poslovanju većinom su u **formatu XML**

e-račun je najrašireniji elektronički poslovni dokument

sve zemlje članice EU trebaju omogućiti primanje e-Računa za porezne svrhe (PDV) ako su ispunjena dva uvjeta:

1) primatelj se mora složiti s primanjem računa u elektroničkom formatu;

2) integritet (nemogućnost izmjene) **i autentičnost** (deklarirani pošiljatelj je stvarni pošiljatelj) moraju biti osigurani pri prijenosu i arhiviranju

Elektronički (digitalni) potpis

Za digitalno potpisivanje koristi se asimetrična kriptografija.

- jedan algoritam i par ključeva: jedan ključ za šifriranje, drugi za dešifriranje
- snaga sustava za šifriranje počiva na ključu
- napadač može imati šifrirane tekstove i znati algoritme, ranjivost sustava ovisi o snazi ključa
- u asimetričnoj kriptografiji ključevi su međusobno vezani
    - neizvedivo je poznavajući algoritam i jedan ključ otkriti drugi
- Svaki korisnik ima **par ključeva**:
    - **privatni** (tajni) **ključ**
        - Dostupan isključivo korisniku, ne smije se distribuirati
    - **javni ključ**
        - Dostupan svima, mora se distribuirati
- Asimetrična kriptografija naziva se i kriptografijom javnog ključa
- Algoritam: **RSA**

Hash funkcija i digitalno potpisivanje

prije digitalnog potpisivanja treba generirati sažetak (hash, digest) poruke

hash funkcija

- ulaz: niz znakova proizvoljne duljine
- izlaz: niz znakova fiksne duljine
- jednosmjerna funkcija (nije moguće na osnovu izlaza regenerirati ulaznu poruku, nije moguće odrediti ulaznu poruku koja bi imala zadani hash)
- Algoritmi: SHA-2, SHA-3, MD5

Digitalni certifikat

- Povezuje identitet korisnika s njegovim javnim ključem - potvrđuje da je određeni korisnik vlasnik određenog javnog ključa
- norma X.509

Sadržaj certifikata

- informacije o korisniku: ime, institucija, država
- jednoznačni serijski broj
- informacija o važenju certifikata
- informacija o povlačenju certifikata
- javni ključ korisnika
- informacija o instituciji koja je izdala certifikat
- digitalni potpis institucije koja je izdala certifikat

Ako pošiljatelj potpiše poruku svojim privatnim ključem, primatelj može znati da se radi upravo o tom pošiljatelju:

- ako može dešifrirati digitalni potpis javnim ključem pošiljatelja i
- ako digitalni certifikat potvrđuje da je korišteni javni ključ upravo javni ključ tog pošiljatelja
- ako digitalni certifikat nije istekao ili opozvan

Infrastruktura javnog ključa

- skup sklopovlja, programske podrške, ljudi, politika i procedura potrebnih za stvaranje, upravljanje, izdavanje, korištenje, pohranjivanje i opozivanje digitalnih certifikata
- osnova za stvaranje sigurne i povjerljive razmjene podataka između sudionika u sustavu
- osigurava:
    - cjelovitost elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom
    - potvrđivanje identiteta strana koje sudjeluju u komunikaciji
    - neporecivost sudjelovanja bilo koje strane u komunikaciji

Dijelovi PKI

- certifikacijsko tijelo
- registracijsko tijelo
- repozitorij
- klijenti (aplikacije)
- korisnici sustava PKI
- centar za pouzdano vremensko označavanje

Hijerarhija certifikacijskih tijela

- Jedan CA može potpisati certifikat drugog CA
- Može se napraviti hijerarhija certifikacijskih tijela (CA)
- Ako nemamo povjerenja u neki CA, možda imamo povjerenja u CA koji je u hijerarhiji iznad njega. Time stječemo povjerenje i u CA na nižoj razini hijerarhije
- CA na najvišoj razini sam potpisuje svoj certifikat – to je onda samopotpisani certifikat. CA sa samopotpisanim certifikatom je korijenski CA

Centar za pouzdano vremensko označavanje (TSA)

Stvara vremenske žigove kako bi se dokazalo da su određeni podaci postojali prije određenog vremena

VREMENSKI ŽIG/PEČAT

Osigurava pouzdanost digitalnog potpisa i poslije isteka valjanosti ili opoziva certifikata potpisnika

- Pomoću vremenskog žiga može se dokazati da je potpis napravljen prije isteka valjanosti certifikata

Postupak provjere vremenskog žiga

Ako su sažetci jednaki, dokazano je da su i vremenska oznaka i dokument nepromijenjeni te da je TSA izdao vremensku oznaku

- Ne može se poreći da je podnositelj zahtjeva za vremenskom oznakom bio u posjedu originalnog dokumenta u vremenu naznačenom vremenskom oznakom.

Ako sažetci nisu jednaki, to znači

- da su vremenska oznaka ili dokument promijenjeni
- da vremensku oznaku nije izdao navedeni TSA

Davatelji usluga certificiranja (CA) u RH

- **Financijska agencija (FINA)**
- **Agencija za komercijalnu djelatnost (AKD)**
- **Zagrebačka banka (ZABA)**

Vremenska ovjera u RH

FINA TSA – davatelj usluga javne vremenske ovjere

- **FINA (kao TSA)** pružatelj je usluge ovjere elektroničkog potpisa
- potvrđuje se da su podaci i elektronički potpis postojali prije stavljanja vremenskog žiga

Digitalni potpis u EU (i RH) – tri vrste potpisa

Elektronički potpis

- podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje

Napredni elektronički potpis mora ispunjavati sljedeće zahtjeve:

- na nedvojben način je povezan s potpisnikom
- omogućava identificiranje potpisnika

- izrađen je korištenjem podataka za izradu elektroničkog potpisa koje potpisnik može, uz visoku razinu pouzdanja, koristiti pod svojom isključivom kontrolom
- povezan je s njime potpisanim podacima na način da se može otkriti bilo koja naknadna izmjena podataka

Kvalificirani elektronički potpis

- napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise

Uredba Eidas

Uredba Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu

Cilj: uspostava povjerenja i uzajamnog priznavanja e-potpisa i epečata unutar EU

Elektronički pečat

Tri vrste pečata:

Elektronički pečat

- podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka

Napredni elektronički pečat mora ispunjavati sljedeće zahtjeve:

- na nedvojben način je povezan s autorom pečata
- omogućava identificiranje autora pečata
- izrađen je korištenjem podataka za izradu elektroničkog pečata koje autor pečata može, uz visoku razinu pouzdanja i pod svojom kontrolom, koristiti za izradu elektroničkog pečata
- povezan je s podacima na koje se odnosi na takav način da se može otkriti bilo koja naknadna izmjena podataka

Kvalificirani elektronički pečat

- napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat

Sigurnost XML-dokumenata

Sigurnosne norme ugrađene u XML:

- XML-Encryption i XML-Signature
- dodaju se dokumentu bez kršenja pravila XML-a
- takvi dokumenti mogu se pregledavati korištenjem standardnih alata za XML

za **siguran prijenos dokumenata** kroz mrežu može se koristiti **protokol TLS**

- time se štiti samo prijenos podataka kroz mrežu, a ne i pohrana
- dokument poslan korištenjem isključivo TLS-a prestaje biti siguran onog trenutka kada stigne na odredište

norma XML Digital Signature koristi se za pohranu digitalnog potpisa u XML dokument

norma XML Encryption koristi se za pohranu kriptiranog sadržaja u formatu XML

Kanonikalizacija

- dva logički jednaka XML-dokumenta mogu biti različito zapisana
- primjerice, u jednom se nalazi razmak viška ili prazan red viška
- kako bi se takvi problemi izbjegli, XML-dokumente treba **kanonikalizirati** tj. svesti se na jednak (kanonički) oblik (normiranje razmaka i sl.)

XML-Signature (XML-DSig)

- XML-DSig je W3C norma
- definira kako ugraditi digitalni potpis u XML dokument (tako da su zadovoljena pravila XML-a)
- nije algoritam za digitalno potpisivanje
- jednim potpisom moguće je potpisati više dokumenata
- moguće je potpisati i dokumente koji nisu u formatu XML
- moguće je potpisati samo dio XML dokumenta

Elementi potpisa:

- XML potpis se u XML dokumentu realizira preko elementa signature
- **Element SignedInfo** – unutar svojih podelemenata identificira podatke koji se potpisuju te različite algoritme koji će se koristiti
- **CanonicalizationMethod** - sadrži ime algoritma kojim se radi kanonikalizacija podataka
- **SignatureMethod** - definira algoritam za generiranje potpisa
- **SignatureValue** - sadrži vrijednost potpisa elementa **SignedInfo**
- **Reference** - identificira resurse koji će biti potpisani i sve algoritme koji će se koristiti za pretprocesiranje podataka. Ti algoritmi su ispisani u elementu **Transforms**

XML potpis može se pojaviti u tri osnovna oblika:

Omotani potpis (Enveloped) – potpis se nalazi unutar dokumenta.

Omotavajući potpis (Enveloping) – potpis omeđuje dokument koji potpisuje.

Odvojeni potpis (Detached) – potpis se nalazi u zasebnom dokumentu, a URI (Universal Resource Identifier) određuje koji dokument potpisuje.

XAdES (XML Advanced Electronic Signatures) - Skup proširenja preporuke XML-Dsig

Definira šest profila koji se razlikuju po razini zaštite koju nude:

XAdES - napredni el. potpis u skladu s Direktivom 1999/93/EC

XAdES-T - uključuje i vremensku oznaku

XAdES-B - dodaje na XAdES-T poveznice na certifikate i listu opozvanih certifikata **XAdES-X** - dodaje na XAdES-C vremenske oznake na uvedene poveznice

XAdES-X-L - u potpisani dokument dodaje certifikate i listu opozvanih certifikata

XAdES-A - zahtijeva slijed vremenskih oznaka za dugoročno arhiviranje

XML Encryption (XML-Enc)

- XML-Enc opisuje kako šifrirani sadržaj ugraditi u XML
- Nije algoritam šifriranja
- Mogu se šifrirati i neXML-ovski dokumenti
- Moguće je šifrirati samo dio XML-dokumenta
- Različite dijelove XML-dokumenta moguće je šifrirati različitim ključevima – kontrola pristupa

Šifriranje se može izvesti na **tri načina**:

korištenjem simetrične kriptografije – podatci se šifriraju simetričnim ključem koji su ranije sudionici komunikacije na neki (siguran) način razmijenili

korištenjem asimetrične kriptografije – podatci se šifriraju javnim ključem primatelja

korištenjem hibridnog pristupa – podatci se šifriraju simetričnim ključem, a taj simetrični ključ šifrira se javnim ključem primatelja; šifrirani simetrični ključ i sadržaj šifriran tim simetričnim ključem ugrađuju se u XML-dokument; ovaj je pristup najučestaliji

Rezultat šifriranja je **podatkovni element** koji sadrži (preko jednog od svojih podelemenata) ili identificira (preko URI reference) šifrirane podatke.

Sigurnosni zahtjevi kod online plaćanja

Autentifikacija - u transakciji online plaćanja se zna tko sudjeluje u transakciji i zna se da je osoba upravo ta za koju tvrdi da jest.

Integritet - podaci iz transakcije se neće mijenjati

Jedinstvenost zahtjeva za plaćanjem - omogućava trgovcu da prepozna ponovni zahtjev za istom transakcijom

Neporecivost transakcije - nakon izvršavanja transakcije kupac ne može poreći da je izvršio transakciju, odnosno trgovac ne može poreći da je primio transakciju

Povjerljivost – podacima o transakciji se ne može neovlašteno pristupiti

Privatnost i anonimnost kupca - trgovac može vidjeti samo pseudonim ili korisničko ime kupca, ali ne i njegove privatne podatke

Pouzdanost sustava - preventivne radnje u slučaju pada sustava te kod greški prilikom izvršavanja transakcije

PCI DSS

- sigurnosni standard za kartično poslovanje
- definira minimalne sigurnosne mjere i procese
- osigurava trgovcima, kartičnim kućama, bankama i ostalim poslovnim subjektima koji se bave kartičnim poslovanjem zaštitu podataka vlasnika kartica
- Banke i pružatelji usluga moraju se certificirati kod kvalificiranih revizora sigurnosti, a trgovci su dužni se pridržavati PCI DSS standarda i obavljati kartično poslovanje samo s certificiranim pružateljima usluga
- PCI DSS regulira zahtjeve koji se odnose na upravljanje sigurnošću podataka, sigurnosne procedure, mrežnu arhitekturu, oblikovanje programske potpore za obradu podataka te ostale kritične zaštitne mjere u kartičnom poslovanju

Neki od zahtjeva:

- **Zahtjev 1:** Instalirati i održavati odgovarajuću konfiguraciju vatrozida (eng. firewall) radi zaštite podataka o vlasnicima kartica
- **Zahtjev 2:** Ne koristiti lozinke i druge sigurnosne parametre dobivene od dobavljača softverskog sigurnosnog rješenja
- **Zahtjev 3:** Svi pohranjeni podatci o vlasniku kartice moraju se uvijek i bezuvjetno štititi
- **Zahtjev 4:** Tijekom prijenosa putem otvorenih, javnih mreža svi podatci o vlasniku kartice moraju se štititi šifriranjem (enkripcijom)
- **Zahtjev 5:** Nužno je koristiti i redovito osvježavati softver za zaštitu od zlonamjernog koda, odnosno antivirusni softver

TLS / SSL

- koristi se za ostvarivanje sigurnije razmjene povjerljivih podataka, poput korisničkog imena i zaporke, broja kreditne kartice i sl.
- temelji se na upotrebi kriptografije te infrastrukture javnih ključeva
- Za kartično plaćanje preko mreže preporučuje se korištenje **TLS**
- onemogućuje se presretanje i neovlašteno prisluškivanje komunikacije te eventualna krađa broja kreditne kartice
- međutim, ne rješava se problem pohrane brojeva kreditne kartice na samom poslužitelju

Phishing - napadači pokušavaju saznati povjerljive podatke (najčešće zaporke, podatke o kreditnoj kartici ili PIN) lažno se predstavljajući kao vjerodostojan subjekt u komunikaciji.

lažnom porukom elektroničke pošte ili porukom preko sustava za trenutno poručivanje korisnika se pokušava namamiti na lažnu web stranicu, kako bi na njoj upisao svoje korisničko ime i zaporku, PIN, broj kreditne kartice i sl.

Korisnik treba vjerovati HTTPS konekciji samo ako:

- Korisnik vjeruje da preglednik ispravno implementira HTTPS s ispravno unaprijed instaliranim provjerama certifikata poznatih i pouzdanih CA
- Sjedište weba ima valjani certifikat (kojeg je potpisao CA)
- Korisnik ima povjerenje u tog CA

TLS/SSL certifikati

- posjetiteljima Web sjedišta potvrđuju identitet web sjedišta,
- garantiraju sigurnu i povjerljivu razmjenu podataka