Osnovni Principi Bezbednosti

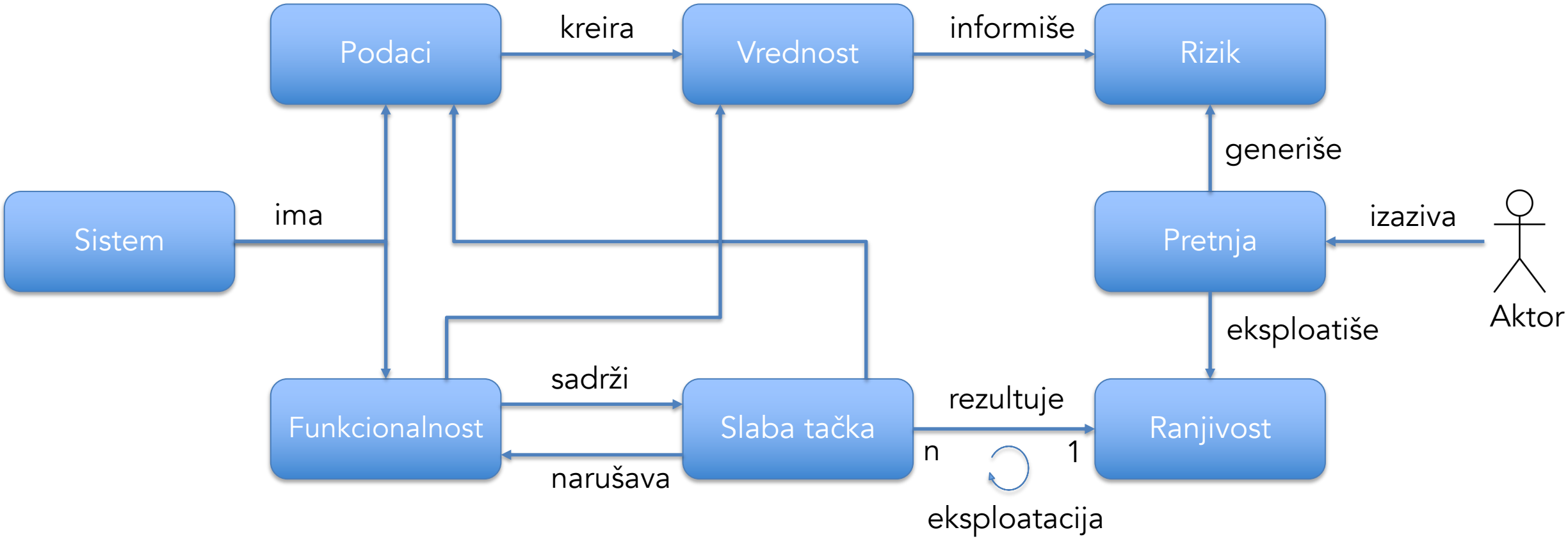
dr Goran Sladić

Sadržaj predavanja

- Osnovni koncepti i terminologija
- Osnovna svojstva
- Osnovne kontrole
- Inženjerstvo bezbednosnih zahteva
- Izvori bezbednosnih zahteva
- Kvalitativni bezbednosni zahtevi
  - Studija slučaja: Slučajevi zloupotrebe
- Eksplicitni bezbednosni zahtevi
  - Studija slučaja: PCI DSS
- Security Assurance Levels (SALs)
- NIST Cybersecurity Framework (CSF)

Osnovni koncepti i terminologija

Osnovni koncepti i terminologija



Slaba tačka (engl. *weakness*)

- Slaba tačka je osnovni nedostatak koji modifikuje ponašanje ili funkcionalnost (što rezultira netačnim ponašanjem) ili dozvoljava neproveren ili netačan pristup podacima
- Slabe tačke u dizajnu sistema su rezultat nepoštovanja najboljih praksi, standarda ili konvencija i dovode do nekog neželjenog efekta na sistem
- Common Weakness Enumeration (CWE)[1] je taksonomija bezbednosnih slabosti i ranjivosti na koje se može pozvati kada se istražuje dizajn sistema

[1] MITRE CWE - https://cwe.mitre.org/data/index.html

Eksploatabilnost (engl. *exploitability*)

- Eksploatabilnost je mera koliko lako napadač može da iskoristi slabu tačku da nanese štetu

- Može se definisati i kao količina izloženosti koju slaba tačka ima spoljašnjem uticaju

Ranjivost (engl. *vulnerability*)

- Kada se slaba tačka može iskoristiti poznata je kao ranjivost
- Predstavlja sredstvo protivniku sa zlom namerom da nanese štetu sistemu
- Ranjivosti koje postoje u sistemu, ali koje su prethodno bile neotkrivene, poznate su kao ranjivosti nultog dana (engl. *zero day*)
- Ranjivosti nultog dana su posebne jer je vrlo verovatno da će biti nerešene na vreme pa je potencijal za eksploataciju veći

Ozbiljnost (engl. *severity*)

- Slabe tačke dovode do uticaja na sistem i njegovu imovinu (funkcionalnost i/ili podatke)

- Potencijal oštećenja od takvog problema opisuje se kao ozbiljnost defekta

Uticaj (engl. *impact*)

- Ako se iskoriste slaba tačka ili ranjivost, to rezultuje nekom vrstom uticaja na sistem, kao što je oštećenje funkcionalnosti ili curenje podataka

- Kada se procenjuje ozbiljnost problema, procenjuje se nivo uticaja kao mera potencijalnog gubitka funkcionalnosti i/ili podataka kao rezultat uspešne eksploatacije

Aktor (engl. *actor*)

- Kada se opisuje sistem, akter je svaka osoba (ili proces) povezana sa sistemom, kao što je korisnik ili napadač

- Učesnik sa zlim namerama, bilo unutrašnjim ili eksternim za organizaciju, koji eksploatiše sistem naziva protivnikom (engl. *adversary*)

Pretnja (engl. *threat*)

- Pretnja je rezultat verovatnoće da će napadač iskoristiti ranjivost da negativno utiče na sistem na određeni način

- Kada protivnik pokuša (uspešno ili ne) da iskoristi ranjivost sa određenim ciljem ili ishodom, to postaje poznato kao pretnja

Gubitak (engl. *loss*)

- Gubitak nastaje kada jedan ili više uticaja pogađa funkcionalnost i/ili podatke kao rezultat toga što je protivnik izazvao pretnju:
  - Aktor je u stanju da utiče na poverljivost podataka kako bi otkrio osetljive ili privatne informacije
  - Aktor može da modifikuje interfejs funkcionalnost, promeni ponašanje funkcionalnosti ili promeni sadržaj ili poreklo podataka
  - Aktor može privremeno ili trajno da spreči ovlašćene entitete da pristupe funkcionalnosti ili podacima

Rizik (engl. *risk*)

- Rizik kombinuje vrednost potencijalno iskorišćenog cilja sa verovatnoćom da se uticaj može ostvariti

- Vrednost se odnosi na vlasnika sistema ili informacije, kao i na napadača

Osnovna svojstva

Poverljivost (engl. *confidentiality*)

- Sistem ima svojstvo poverljivosti samo ako garantuje pristup podacima koji su mu povereni isključivo onima koji imaju odgovarajuća prava, na osnovu njihove potrebe da poznaju zaštićenu informaciju[1]
- Sistem koji nema barijeru koja sprečava neovlašćeni pristup ne uspeva da zaštiti poverljivost

[1] NIST 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations: B-5

Integritet (engl. *integrity*)

- Integritet postoji kada se autentičnost podataka ili operacija može proveriti, a podaci ili funkcionalnost nisu modifikovani ili učinjeni neautentičnim neovlašćenom aktivnošću[1]

[1] NIST 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations: B-12

Dostupnost (engl. *availability*)

- Dostupnost znači da su ovlašćeni aktori u mogućnosti da pristupe funkcionalnosti sistema i/ili podacima kad god za to imaju potrebu ili želju[1]
- U određenim okolnostima, podaci ili operacije sistema možda neće biti dostupni kao rezultat ugovora ili sporazuma između korisnika i operatera sistema
- Ako je sistem nedostupan zbog zlonamerne akcije protivnika, dostupnost će biti ugrožena

[1] NIST 800-160 vol 1, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems": 166

Sigurnost (engl. *safety*)

- Sigurnost znači da nije prouzrokovana nikakva šteta — namerna ili na neki drugi način
- Bezbednost znači da nije prouzrokovana namerna šteta — uopšte

Osnovne kontrole

Identifikacija (engl. *identification*)

- Akterima u sistemu se mora dodeliti jedinstveni identifikator koji ima značenje za sistem
- Identifikatori bi takođe trebali biti značajni za pojedince ili procese koji će koristiti identitet
- Učesnik je bilo šta u sistemu (uključujući ljudske korisnike, sistemske naloge i procese) što ima uticaj na sistem i njegove funkcije, ili što želi da dobije pristup podacima sistema
- Da bi podržao mnoge bezbednosne ciljeve, akteru se mora dodeliti identitet pre nego što može da radi na tom sistem
- Ovaj identitet mora da dolazi sa informacijama koje omogućavaju sistemu da pozitivno identifikuje aktera

Autentifikacija (engl. *authentication*)

- Aktori sa identitetima treba da dokažu svoj identitet sistemu
- Identitet se dokazuje upotrebom kredencijala (npr.lozinka ili sigurnosni token)
- Svi aktori koji žele da koriste sistem moraju biti u mogućnosti da na zadovoljavajući način dostave dokaz svog identiteta kako bi ciljni sistem mogao da potvrdi da komunicira sa pravim aktorom
- Autentifikacija je preduslov za autorizaciju

Autorizacija (engl. *authorizaton*)

- Kada je aktor autentifikovan mogu mu se dodeliti privilegije unutar sistema za obavljanje operacija ili pristup funkcionalnosti ili podacima
- Autorizacija je kontekstualna i može biti, ali nije obavezna, tranzitivna, dvosmerna ili recipročna po prirodi
- Šeme kontrole pristupa koje upravljaju ponašanjem aktora u sistemu mogu biti razne:
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Attribute-based access control (ABAC)
  - Capability-based access control (CapBAC)
  - Itd.

Logovanje (engl. *logging*)

- Kada aktor izvrši sistemsku operaciju, kao što je izvršavanje funkcije ili pristup skladištima podataka, log tog događaja treba da se zapiše
- Ova aktivnost obezbeđuje praćenje izvršenih operacija
- Kada se zabeleženi događaji smatraju bezbednosno relevantnim, mogu se koristiti za kritične zadatke kao što su otkrivanje i prevencija napada, forenzika i prikupljanje dokaza o napadu

Revizija (engl. *auditing*)

- Logovanje stvara zapise (engl. *logs*)
- *Audit* logovi su dobro definisani (u formatu i sadržaju), poređani po vremenu i obično otporni na neovlašćeno korišćenje
- Sposobnost da se pogleda u prošlost i razume redosled po kome su se događaji desili, ko je izvršio koje operacije i kada, i opciono da se utvrdi da li su operacije bile ispravne i autorizovane, ključna je za bezbednosne operacije i odgovor na incidente

Inženjerstvo bezbednosnih zahteva

Inženjerstvo bezbednosnih zahteva

- Bezbednosni zahtevi se smatraju nefunkcionalnim, kvalitativnim zahtevma
- Inženjerstvo bezbednosnih zahteva istražuje zaštitu imovine od potencijalnih pretnji koje mogu da dovedu do štete
- Pristupi inženjeristvu bezbednosnih zahteva mogu se podeliti u četiri klase[1]:
  - Zasnovani na ciljevima
  - Zasnovani na modelu
  - Orijentisani na probleme
  - Procesno orijentisani

[1] Nhlabatsi et al. Security requirements engineering for evolving software systems: A survey. 2012.

Pristupi zasnovani na ciljevima

- Koriste ciljeve da bi obuhvatili bezbednosne zahteve:
  - Secure Tropos[1]
    - Proširuje metode razvoja softvera zasnovane na paradigmi razvoja softvera orijentisanog na agente pod nazivom Tropos sa bezbednosnim konceptima kao što su:
      - Bezbednosna ograničenja
      - Zavisnosti
      - Ciljevi
      - Bezbedni entiteti
    - Bezbednosna ograničenja se mogu tumačiti kao bezbednosni uslovi ili zahtevi koje korisnici ne mogu da ignorišu, ali tumače kao prepreku koja ograničava postizanje ciljeva korisnika
  - Metoda **Anti-Models**[2]
    - Gradi dva konkurentna modela:
      - Željeni model sistema
      - Anti-model sa ranjivostima potrebnim za postizanje anti-ciljeva
    - Kombinuje nalaze kako bi obogatio sistem sa novim bezbednosnim zahtevima
    - Proširuje sticanje znanja u okviru automatizovane specifikacije (KAOS) za ciljno orijentisano inženjerstvo zahteva
      - Npr., novim obrascima za formalno otkrivanje bezbednosnih zahteva i principom dualnosti za modeliranje pretnji

[1] Mouratidis H. et al. Secure tropos: a security-oriented extension of the tropos methodology. 2007.
[2] Van Lamsweerde A. Elaborating security requirements by construction of intentional anti-models. 2004.

Pristupi zasnovani na modelu

- Zagovaraju da modeli pomažu analitičarima zahteva da razumeju probleme softvera i identifikuju potencijalna rešenja koristeći apstrakcije
- Dva istaknuta predstavnika su UMLSec i SecureUML
- **UMLSec** je UML ekstenzija koja omogućava korisnicima da dodaju bezbednosne stereotipe i ograničenja u dizajn sistema[1]
  - Može se koristiti za procenu specifikacija UML sistema za ranjivosti koristeći formalnu semantiku
  - UMLSec je korišćen kao osnova za CARiSMA alat[2] koji može da obogati model sistema bezbednosnim zahtevima fokusirajući se na poverljivost, integritet i karakteristike dostupnosti kako bi se izvršila bezbednosna analiza
- **SecureUML** je UML ekstenzija koja koristi smernice za kontrolu pristupa zasnovane na ulogama (RBAC) za definisanje i sprovođenje ograničenja autorizacije u modelovanim sistemima zasnovanim na UML-u[3]

[1] Jujens J. UMLsec: Extending UML for secure systems development. 2002.
[2] Ahmadian A. et al. Model-based privacy and security analysis with CARiSMA. 2017.
[3] Lodderstedt T. et al SecureUML: A UML-based modeling language for model-driven security. 2002.

Pristupi orijentisani na probleme

- Pružaju alate za analizu problema razvoja softvera
- Jedan primer su okvire zloupotrebe (engl. ***abuse frames***) i antizahteva[1]
- Za razliku od okvira rešavanja problema (engl. *problem frames*) koji se fokusiraju na odbrambene zahteve koji moraju biti zadovoljeni, anti-zahtevi definišu namere zlonamernih korisnika koje moraju biti sprečene
- Autori integrišu anti-zahteve u okvire zloupotrebe da bi predstavljali bezbednosne pretnje i iz njih izveli zahteve
- ***Misuse cases*** su još jedan primer ovog pristupa[2]
- Predstavljaju negativnu formu slučajeva upotrebe (engl. *use cases*), tj. slučajeve upotrebe koji mogu negativno uticati na sistem

[1] Lin et al. Introducing abuse frames for analysing security requirement. 2003.
[2] Alexander I. Initial industrial experience of misuse cases in trade-off analysis. 2002.

Procesno orijentisani pristupi

- Fokusiraju se na procese u više koraka za analizu bezbednosnih zahteva
- **System Quality Requirement Engineering** (SQUARE) je model procesa u devet koraka razvijen na Univerzitetu Carnegie Mellon kako bi se obezbedila sredstva za izazivanje, kategorizaciju i davanje prioriteta bezbednosnim zahtevima za sisteme i aplikacije informacionih tehnologija[1]
- Ideja iza SQUARE-a je da se ugrade koncepte bezbednosti u rane faze životnog ciklusa razvoja, a ne naknadno
- Jedan od koraka zahteva procenu rizika jer može pomoći da se identifikuju bezbednosne izloženosti visokog prioriteta
- Drugi primer je **metodologija zasnovana na aspektno orijentisanom modeliranju za ugrađivanje bezbednosnih mehanizama** u aplikaciju koristeći aktivnosti kao što su analiza rizika i generisanje *misuse* modela[2]

[1] Mead N. et al. Security quality requirements engineering (SQUARE) methodology. 2005.
[2] Georg G. et al. An aspect-oriented methodology for designing secure applications. 2009.

Izvori bezbednosnih zahteva

Poslovni zahtevi vs softverski zahtevi

- Poslovni zahtevi se odnose na poslovne ciljeve, viziju i ciljeve i obezbeđuju obim poslovne potrebe ili problema koji treba da se reši kroz određenu aktivnost ili projekat
- Softverski zahtevi razlažu korake specifične za softver koji su potrebni za ispunjavanje poslovnih zahteva
- Poslovni zahtev navodi „zašto“ za projekat, dok zahtevi softvera navode „šta“

Inženjerstvo zahteva 1/2

- Softverski zahtev je sposobnost softvera da korisniku reši problem ili da postigne određeni cilj
- Inženjerstvo zahteva je proces definisanja očekivanja korisnika za novi softver koji se razvija ili modifikuje
- Glavni izazov za softver inženjere je da podele viziju finalnog proizvoda sa klijentom – svi akteri u projektu moraju da postignu zajedničko razumevanje o tome šta će proizvod biti i šta će raditi
- Potreban je način da se precizno definišu, razumeju i predstave želje klijenta kada se definišu zahtevi za softverski proizvod

Inženjerstvo zahteva 2/2

- Zahtevi treba da budu dokumentovani, izvodljivi, merljivi, da se mogu testirati, sledljivi (tracable), povezani sa identifikovanim poslovnim potrebama ili mogu□nostima i definisani do nivoa detalja koji je dovoljan za dizajn softvera
- Inženjerstvo zahteva obuhvata tri aktivnosti:
  - Izdvajanje (selekcija) zahteva – komunikacija sa klijentima i korisnicima kako bi se utvrdile njihove potrebe
  - Analiziranje zahteva – utvrđivanje da li su navedeni zahtevi nejasni, nepotpuni, dvosmisleni ili kontradiktorni, a zatim rešavanje ovih pitanja
  - Modeliranje zahteva – zahtevi mogu biti dokumentovani u različitim oblicima, kao što su dokumenti na prirodnom jeziku, slučajevi koriš□enja, korisničke priče ili specifikacije

Izdvajanje (selekcija) bezbednosnih zahteva

- Klijent (obično) ne poseduje dovoljno znanja da postavi specifične bezbednosne zahteve softvera
  - Klijent će navesti da funkcija X treba da se izvrši kada pritisne dugme Y
  - Klijent neće navesti da funkcija X treba da bude otporna na injection napade
- Klijent može da definiše bezbednosne zahteve visokog nivoa
  - Izbeći regulatorne kazne (definisano kroz regulatorna dokumenta)
  - Održavati nesmetano funkcionisanje sistema
  - Očuvati poverenje kupaca i partnera
  - Zaštiti integritet brenda

Analiza bezbednosnih zahteva

- Analiza bezbednosnih zahteva podrazumeva dekomponovanje zahteva poslovne bezbednosti na odluke o dizajnu i implementacione taskove za softver
- "Odlučiti šta treba zaštititi i kako to učiniti"
  - Kako znati da je nešto zaštićeno?
- Bezbednosni zahtevi se ispituju iz dve perspective
  - Granularnost: visoki nivo i niski nivo
  - Izvor: eksplicitni i kvalitativni

Klasifikacija bezbednosnih zahteva: granularnost

- Visko nivo
  - Bazirano na CIA trijadi AAA kontrolama (authentication, authorization, auditing)
  - Obezbediti poverljivosti PII
  - Kontrolisati pristup PII
- Nizak nivo
  - Mapiranje na programski kod i konfiguracije
  - Izvršiti sprovođenje kontrole pristupa na funkciji čitanja PII po principu najmanjih privilegija
  - Šifrovati PII tokom transporta između servisa A i servisa B
  - Izvršiti validaciju unosa za sve podatke koji se šalju u bazu podataka u kojoj se čuvaju PII

Klasifikacija bezbednosnih zahteva: izvor

- Kvalitativni bezbednosni zahtevi
  - Izvedeni iz ispitivanja sistema iz perspektive napadača (npr. modeliranje pretnji, slučajevi zloupotrebe, …)
  - Granularnost zavisi od cilja analize (npr. visoki nivo za arhitekturu sistema, niski nivo za korisničke priče)
  - Identifikacija i analiza u velikoj meri zavise od stručnosti bezbednosnog analitičara
- Eksplicitni bezbednosni zahtevi
  - Mapirano na autoritativne dokumente (npr. zakoni o sajber bezbednosti, propisi, standardi)
  - Mogu biti visokog nivoa (npr. kontrola pristupa zdravstvenim informacijama) ili niskog nivoa (npr. lozinke treba da imaju najmanje 8 znakova)
  - Obično ih je lakše identifikovati, implementirati, testirati i revidirati

Kvalitativni bezbednosni zahtevi

Kvalitativni bezbednosni zahtevi

- Jedan način je da se definišu kroz model pretnji
- Model pretnji je krovni termin za tehnike bezbednosne analize dizajnirane da se razume:
  - Šta napadač želi da postigne (pretnja)
  - Kako to može da postigne (napad)
  - Kako sistem može da ga spreči (ranivosti, mere zaštite)
- Kvalitet modela pretnje zavisi od bezbednosne ekspertize korisnika koji je sporvodi i tačnog razumevanja sistema
- Model pretnji može da se uradi za bilo koji sistem (npr. fizički, digitalni) i na bilo kom nivou granularnosti (npr. sistem preduzeć?a, softverska aplikacija, API)

Model pretnji

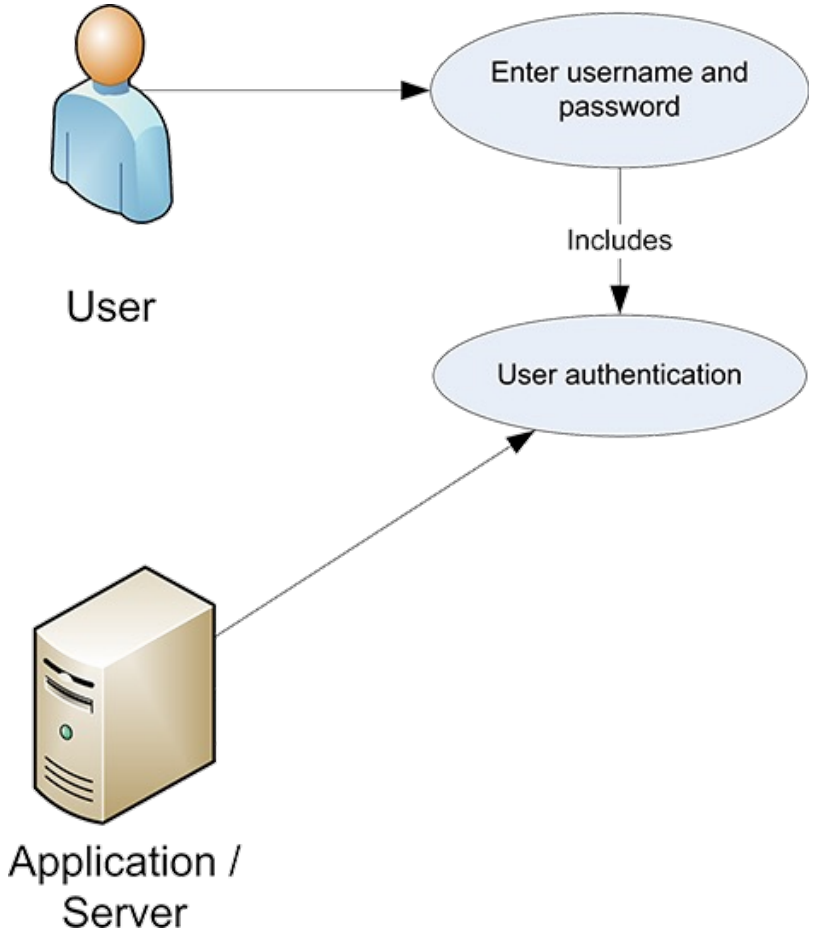
- Postoje mnoge tehnike, ali je većina bazirana na sledećim koracima:
  1. Identifikacija kritičnih aseta (npr. informacije, lokacije, sistemske funkcije)
  2. Definisanje bezbednosnih ciljeva za svaki aset (npr. poverljivost, integritet, dostupnost)
  3. **Identifikovanje i razlaganje pretnji za svaki bezbednosni cilj**
  4. Identifikacija i analiza rizika
  5. **Definisati bezbednosne zahteve za mitigaciju pretnji**

Studija slučaja: Slučajevi zloupotrebe

Attacker-Centric Use Cases

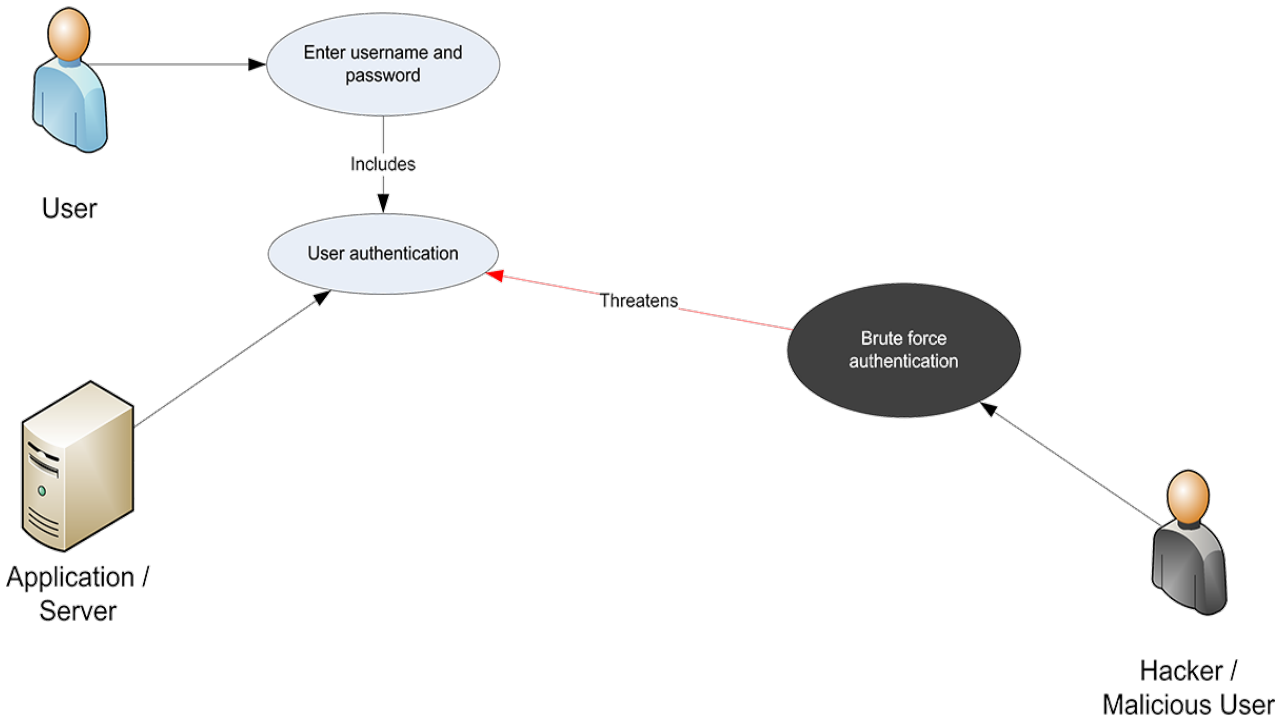
Slučaj korišćenja

- Slučajevi korišc?enja su način određivanja, komuniciranja, specificiranja i dokumentovanja softverskih zahteva
- Slučaj korišćenja je lista radnji ili događaja koji obično definišu interakciju između određene korisničke uloge i sistema radi postizanja cilja
- Jednostavniji za opis aktivnosti u odnosu na deklarativne specifikacije



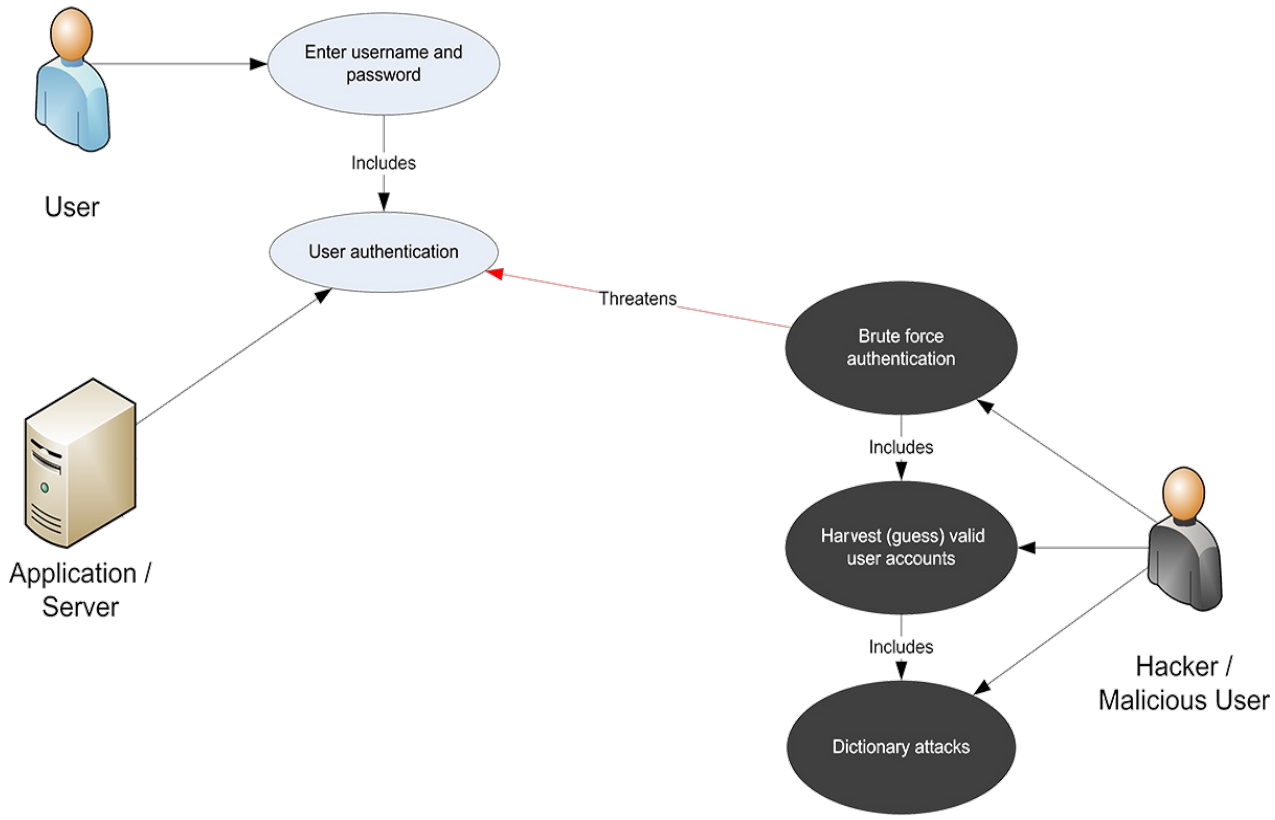
Slučaj zloupotrebe - koncept 1/3

- Slučaj zloupotrebe je niz radnji koje sistem ili drugi entitet mogu da izvrše dok komuniciraju sa malicioznim korisnicima i nanose štetu nekoj zainteresovanoj strani ako se ove radnje uspešno završe
- Slučajevi zloupotrebe ugrožavaju slučajeve korišćenja, što znači da se slučaj korišćenja iskorišćava ili ometa slučajem zloupotrebe



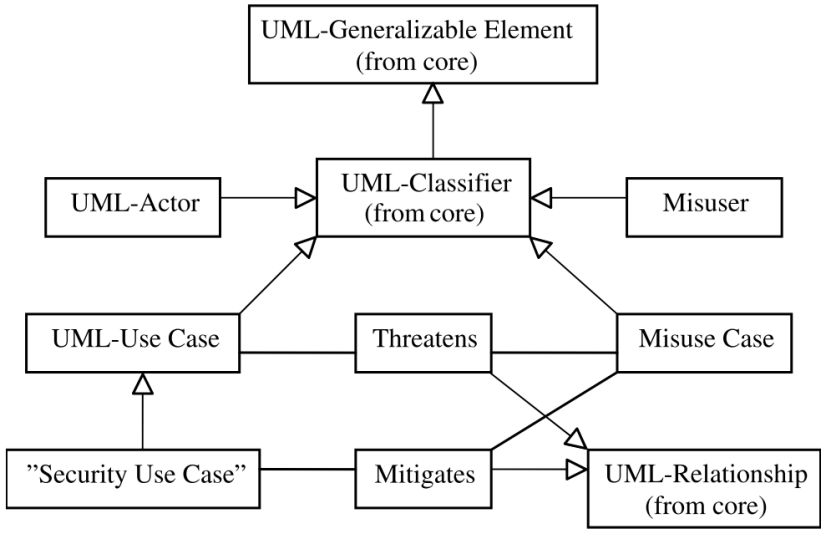
Slučaj zloupotrebe - koncept 2/3

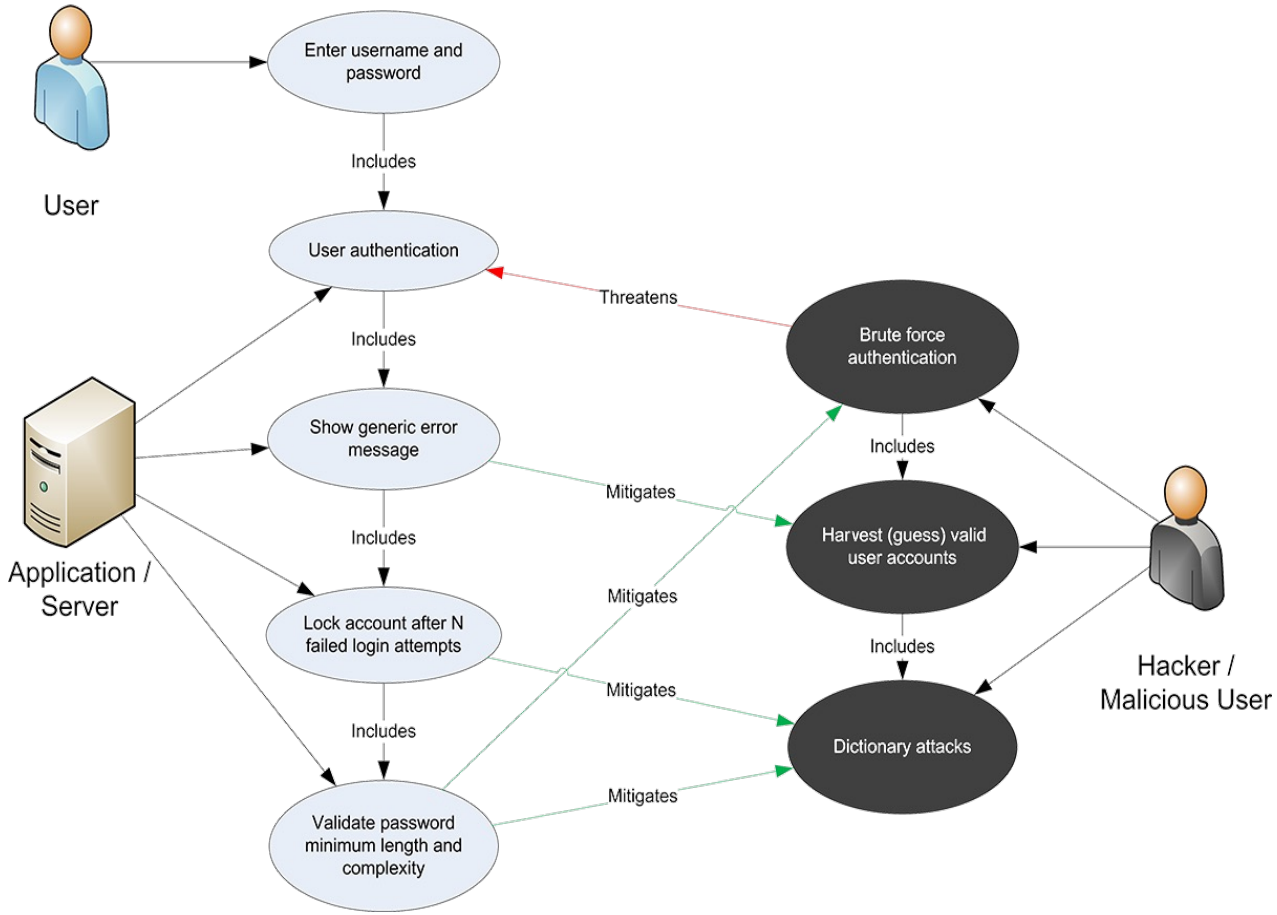
- Relacija **asocijacije** se koristi između malicioznog korisnika i njegovog slučaja zloupotrebe
- Standardne relacije iz slučajeva korišćenja (**include**, **extend**, i **generalize**) se mogu koristiti i između slučajeva zloupotrebe



Slučaj zloupotrebe - koncept 3/3

- Slučaj korišćenja može **mitigovati** slučaj zloupotrebe time što će smanjiti šansu slučaja zloupotrebe da uspe – **bezbednosni slučaj korišćenja**





Zloupotreba ATM

1. Koji su slučajevi korišćenja?
   - Koji su sve aseti dostupni?
   - Šta su njihovi bezbednosni ciljevi?
2. Koji su slučajevi zloupotrebe?
   - Ko su mailiciozni korisnici?
3. Koji su bezbednosni slučajevi korišćenja?

Abuser Stories

- *Abuser stories* su za user stories ono što su slučajevi zloupotrebe za slučajeve korišćenja
- *Abuser stories* identifikuju kako napadači mogu da zloupotrebe sistem i ugroze imovinu zainteresovanih strana
- *As a hacker I want to steal credit card information so that I can make fraudulent charges*
- (Kao haker želim da ukradem podatke o kreditnoj kartici kako bih mogao da izvršim lažne naplate)

Eksplicitni bezbednosni zahtevi

Standardi vs. regulative

- **Standard** sajber bezbednosti je dokument odobren konsenzusom od strane priznatog (standardizacionog) tela, koji obezbeđuje pravila, smernice ili karakteristike za zaštitu proizvoda od sajber napada, a sa kime **usklađenost nije obavezna**
  - ISO 27001, IEC 62443
- **Propis (regulativa)** o sajber bezbednosti sadrži direktive koje štite informacionu tehnologiju i računarske sisteme, dajući uputstva kompanijama i organizacijama da štite svoje sisteme i informacije od sajber napada, pri čemu je **usklađenost obavezna**
  - GDPR, NERC CIP

Studija slučaja: PCI DSS

Payment Card Industry Data Security Standard

Pregled 1/2

- Tehnički standard koji ima za cilj da zaštiti poverljivost podataka o debitnoj i kreditnoj kartici (cardholder data, CHD)
- Cilj je sprečiti prevaru sa platnim karticama, obezbeđivanjem CHD u organizacijama koje prihvataju plaćanja karticama ili rukuju podacima o vlasnicima kartica
- Sastoji se od 12 grupa zahteva koji se fokusiraju na:
  - Ljude i procese organizacije (dokumenti, procedure, awareness)
  - Tehnički sloj IT infrastrukture (mreža, zaštitni zid, operativni sistem, antivirus)
  - Tehnički nivo aplikativnog softvera

Pregled 2/2

Zahtevi	Odgovoran
1. Instalacija i održavanje firewall konfiguracije	IT
2. Ne koristiti podrazumevane vrednosti za bezbednosne parametrekoje je obezbedio proizvođač	IT
3. Zaštita sačuvanih CHD	IT, Development
4. Šifrovanje prenosa CHD-a preko otvorenih javnih mreža	IT, Development
5. Koristiti i redovno ažurirati antivirusni softver	IT
6. Razvoj i održavavanje bezbednih sistema i aplikacija	Development
7. Ograničite pristup CHD-u prema poslovnoj potrebi	IT, Development
8. Dodelite jedinstveni ID svakoj osobi koja pristupa podacima	IT
9. Ograničite fizički pristup CHD	IT
10. Pratiti i nadgledati sav pristup mrežnim resursima i CHD-u	IT, Development
11. Redovno testirati bezbednosne sisteme i procese	IT, QC
12. Održavajte politiku bezbednosti za svo osoblje	Management

Zahtev. 3: Zaštita sačuvanih CHD

- 3.1 Čuvati minimum potrebih CHD implementacijom procesa zadržavanja i odlaganja podataka (*data retention and disposal*) - uključujući i nivo softvera
- 3.2 Ne čuvajte osetljive podatke za autentifikaciju nakon autorizacije (CVV, PIN)
- 3.3 Maskirajte PAN kada se prikaže (max prvih šest i poslednje četiri cifre)
- 3.4 Učiniti PAN nečitljivim bilo gde da se čuva (kriptografija)
- 3.5, 3.6 Zaštititi kriptografske ključeve i osigurati bezbedno upravljanje
- 3.7 Sve dokumentovati

Zahtev 4: Šifrovati prenos CHD

- 4.1 Koristite snažnu kriptografiju i bezbednosne protokole da bi zaštitili osetljive CHD tokom prenosa preko otvorenih, javnih mreža
- 4.2 Nikada ne slati nezaštićene PAN-ove putem tehnologija za razmenu poruka krajnjih korisnika (e-pošta, trenutne poruke, SMS, chat, itd.)
- 4.3 Sve dokumentovati

Zahtev 6: Razvoj i održavavanje bezbednih sistema 1/3

- 6.1 Uspostaviti proces za identifikaciju bezbednosnih ranjivosti, koristeći renomirane spoljne izvore za informacije o ranjivostima i dodeljivanje nivoa rizika
  - Operativni sistem, firmver uređaja, infrastrukturni alati, softverske biblioteke
- 6.2 Verifikovati da su sve komponente sistema i softvera zaštićeni od poznatih ranjivosti instalacijom primenljivih bezbednosnih pečeva
  - Operativni sistem, firmver uređaja, infrastrukturni alati, softverske biblioteke

Zahtev 6: Razvoj i održavavanje bezbednih sistema 2/3

- 6.3 Razvijati interne i eksterne aplikacije (uključujući veb-bazirani administrativni pristup aplikacijama) bezbedno:
  - U skladu sa PCI DSS (bezbedna autentifikacija, logovanje, hardenovanje)
  - Na osnovu industrijskih standarda i najboljih praksa
  - Uključivanje bezbednosti u SDLC (modeliranje pretnji, code review)
- 6.4 Pratiti procese kontrole izmena za sve ismene svih komponenti sistema
  - Odvojiti razvojno/testno okruženje od produkcionog okruženja
  - Produkcioni podaci (npr. stvarni PAN-ovi) se ne koriste za testiranje ili razvoj
  - Uklanjanje testnih podataka i naloga sa sistema pre go live faze

Zahtev 6: Razvoj i održavavanje bezbednih sistema 2/3

- 6.5 Ukloniti/pratiti uobičajene ranjivosti koje nastaju tokom kodiranja
  - Injection flaws, cross-site scripting, autentifikacija i autorizacija, obrada grešaka…
  - Na osnovu industrijskih standarda i najbolje prakse (OWASP, SANS, CERT…)
- 6.6 Za javno dostupne veb aplikacije, stalno pratiti nove pretnje i ranjivosti i osigurati zaštitu od poznatih napada
  - Koristiti automatizovane testove i alate za skeniranje ranjivosti aplikacija
- 6.7 Sve dokumentovati

Zahtev.7: Ograničite pristup CHD

- 7.1 Ograničite pristup komponentama sistema i CHD samo na one pojedince čiji posao zahteva takav pristup
- 7.2 Uspostaviti sistem kontrole pristupa za komponente sistema koji ograničava pristup na osnovu minimalnih potreba pristupa korisnika i koji je podešen na "*deny by default*"
- 7.3 Sve dokumentovati

Zahtev 10: Pratiti i nadgledati pristup CHD-u

- 10.1 Implementirati audit trails kako bi se ispratili pristupi svako korisnika
- 10.2 Implementirati audit trails da se mogu rekonstruisati bitni događaji
- 10.3 Implementirati audit trails da sadrže sve bitne podatke o događaju
- 10.4 Sinhronizacija časovnika
- 10.5 Bezbednosni audit trails
- 10.6 Implementirati log monitoring
- 10.7 Sačivati audit trail istoriju
- 10.8 Sve dokumentovati

Zaključak

- PCI DSS je tehnički standard koji ima za cilj da zaštiti samo poverljivost podataka o debitnoj i kreditnoj kartici (cardholder data)
- Nije dovoljan da obuhvati celokupnu bezbednosnu politiku organizacije
- Većina PCI DSS zahteva može se naći u vodećim industrijskim standardima i najboljim praksama
- Većina zahteva za razvoj softvera pokrivena je elementarnim bezbednosnim konceptima – kriptografijom, kontrolom pristupa, validacijom i logovanjem

Security Assurance Levels (SALs)

Security Assurance Levels (SALs)

- Koncept vektora nivoa sigurnosti sigurnosti (SALs) koji opisuje zaštitni faktor potreban da bi se osigurala bezbednost sistema[1]
- SAL-ovi imaju za cilj da pomognu programerima, korisnicima i kreatorima standarda da razumeju zaštitni faktor bez ulaženja u detalje o svakom standardu pojedinačno
- Oni predstavljaju kvalitativni pristup rešavanju bezbednosti sistema podeljenog na zone
- SAL-ovi se mogu podeliti na četiri različita tipa koji se mogu koristiti u različitim fazama životnog ciklusa bezbednosti:
  - Target SAL - predstavlja željeni nivo sigurnosti za sistem
  - Design SAL - predstavlja planirani nivo sigurnosti za sistem
  - Achieved SAL - predstavlja stvarni nivo sigurnosti za sistem
  - Capability SAL - predstavlja nivo bezbednosti koji sistem može da dostigne ako je pravilno konfigurisan

[1] Gilsinn J. D., et al. Security assurance levels: a vector approach to describing security requirements.

Security Assurance Levels (SALs)

- Ovi SAL-ovi su zasnovani na sedam osnovnih zahteva koji su definisani u standardima *International Electrotechnical Commission* (IEC) 62443:
  - Kontrola pristupa
  - Kontrola upotrebe
  - Integritet podataka
  - Poverljivost podataka
  - Ograničavanje protoka podataka
  - Pravovremeni odgovor na događaj
  - Dostupnost resursa

Security Assurance Levels (SALs)

- Ovde SAL-ovi nisu izraženi kao jedan broj već kao vektor vrednosti koji odgovaraju sedam osnovnih zahteva
- SAL-ovi su definisani u četiri nivoa, gde svaki nivo povećava bezbednosni položaj:
  - SAL 1 - opisuje zaštitu od slučajnog kršenja kontrola. Ova kršenja kontrola (obično labave politike i procedure) mogu doći i od zaposlenih i od spoljnih napadača.
  - SAL 2 - opisuje zaštitu od namernog kršenja kontrola korišćenjem jednostavnih sredstava. Ova sredstva ne zahtevaju mnogo detalja o bezbednosti sistema.
  - SAL 3 - opisuje zaštitu od namernog kršenja kontrola korišćenjem sofisticiranih sredstava. Ovde napadači zahtevaju napredno znanje o bezbednosti određenog sistema da bi napravili prilagođene napade.
  - SAL 4 - opisuje zaštitu od namernog kršenja kontrola korišćenjem sofisticiranih sredstava sa proširenim resursima
- Razlika između SAL 3 i SAL 4 je u resursima koje napadači imaju na raspolaganju

NIST Cybersecurity Framework (CSF)

Komponente radnog okvira

- NIST Cibersecurity Framework (CSF) definiše jedan pogled kroz koji se mogu analizirati bezbednosni zahtevi[1]
- CSF je pristup upravljanja rizikom od sajber bezbednosti zasnovan na riziku
- Tri glavne komponente okvira:
  - Nivoi implementacije radnog okvira
  - Jezgro radnog okvira
  - Profili radnog okvira

[1] NIST Cybersecurity Framework (CSF) - https://www.nist.gov/cyberframework

Nivoi implementacije radnog okvira

- Opisuje kako organizacija upravlja rizikom od sajber bezbednosti
- Opisuje stepen do kojeg prakse upravljanja rizicima u sajber bezbednosti organizacije pokazuju ključne karakteristike (npr. svesnost rizika i pretnji, ponovljiva i prilagodljiva)
- Opcije nivoa: delimični (nivo 1), informisani o riziku (nivo 2), informisani o riziku i ponovljivi (nivo 3), adaptivni (nivo 4)
- Svaka organizacija odlučuje koji nivo odgovara njenim potrebama i mogućnostima upravljanja rizikom

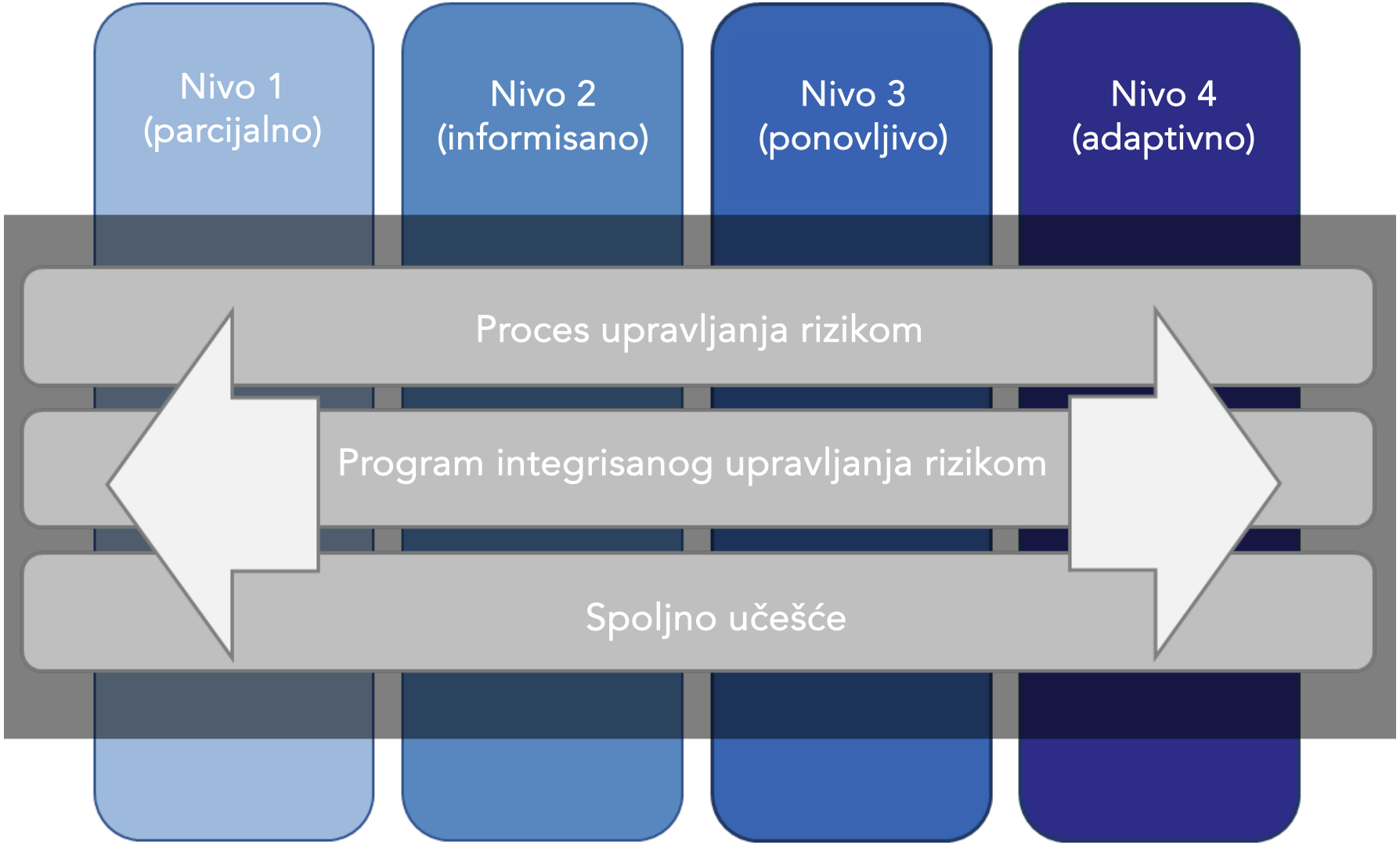
Jezgro radnog okvira

- Aktivnosti sajber bezbednosti i informativne reference, organizovane oko određenih ishoda.Omogućava komunikaciju o sajber rizika u celoj organizaciji.
- Sastoji se od funkcija, kategorija, potkategorija i informativnih referenci
- Funkcije: Identifikacija, Zaštita, Sprečavanje, Odgovor, Oporavak

Profili radnog okvira

- Usklađuje industrijske standarde i najbolje prakse sa jezgrom okvira u određenom scenariju implementacije
- Podržava određivanje prioriteta i merenje uz uvažavanje poslovnih potreba
- Pomaže organizacijama da napreduju sa trenutnog nivoa sofisticiranosti sajber bezbednosti do ciljanog poboljšanog stanja

Implementacioni nivoi



Framework Core

Koji procesi i imovina zahtevaju zaštitu?

Koje mere zaštite su dostupne?

Koje tehnike mogu da identifikuju incidente?

Koje tehnike mogu suzdržati uticaje na incidente?

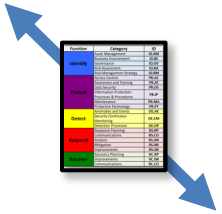
Koje tehnike mogu da povrate sposobnosti?

Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
	Supply Chain Risk Management	**ID.SC**
Protect	Identity Management & Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Core – prevodilački sloj

Senior rukovodioci

- Mišljenja odbora
- Apstrahovani rečnik rizika



Specijalisti u drugim poljima

- Spcifičan fokus van polja bezbednosti
- Specijalizovan ili nikakav rečnik poznavanja rizika

Implementacija / operacije

Temeljno tehničo mišljenje
Visoko specijalizovani rečnik

Potkategorije i informativne reference

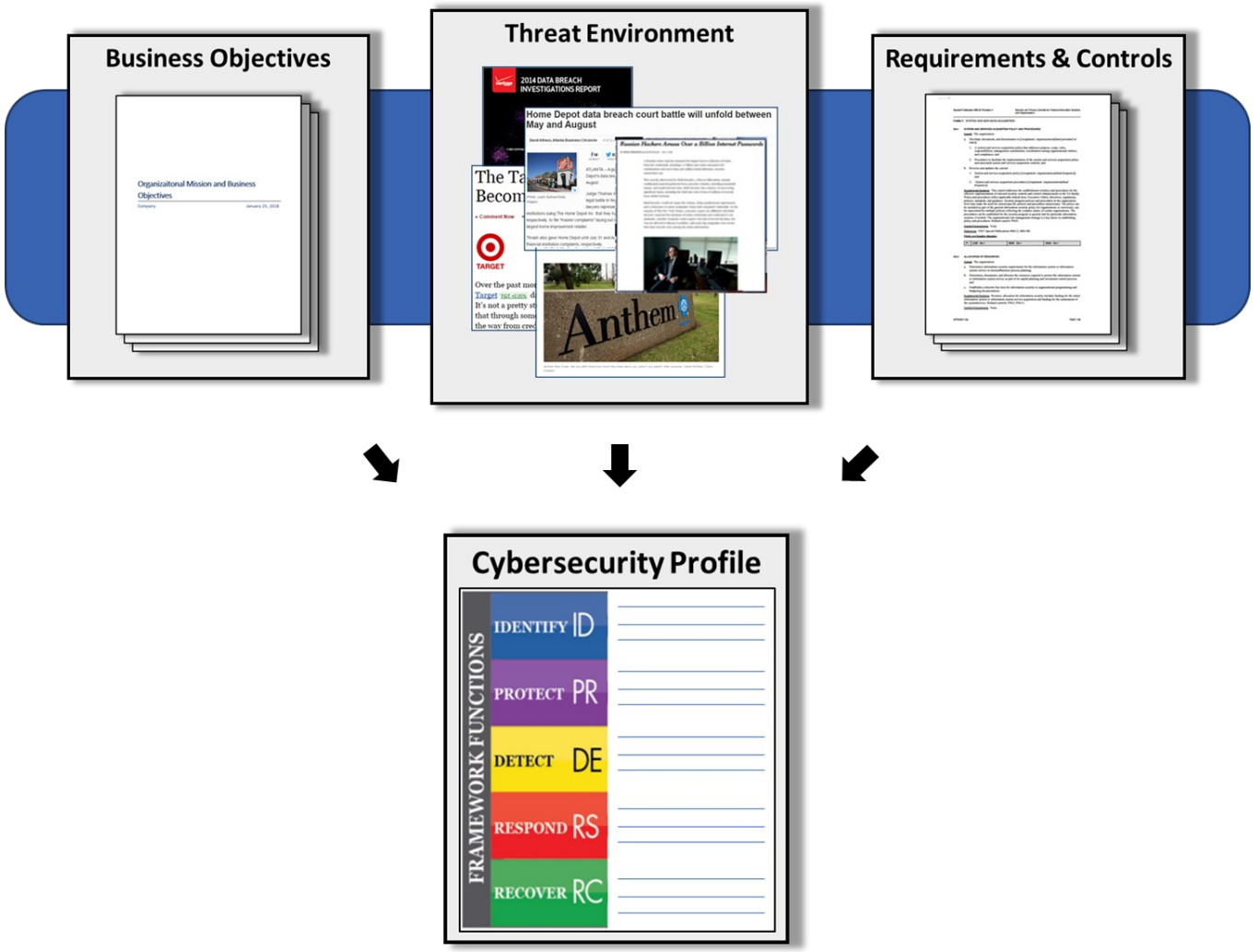
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Profili radnog okvira

- Usklađivanje funkcija, kategorija i potkategorija sa poslovnim zahtevima, tolerancijom na rizik i resursima organizacije
- Omogućava organizacijama da uspostave mapu puta za smanjenje rizika
- Koristi se da opiše **trenutno stanje** ili **željeno ciljno stanje** aktivnosti sajber bezbednosti

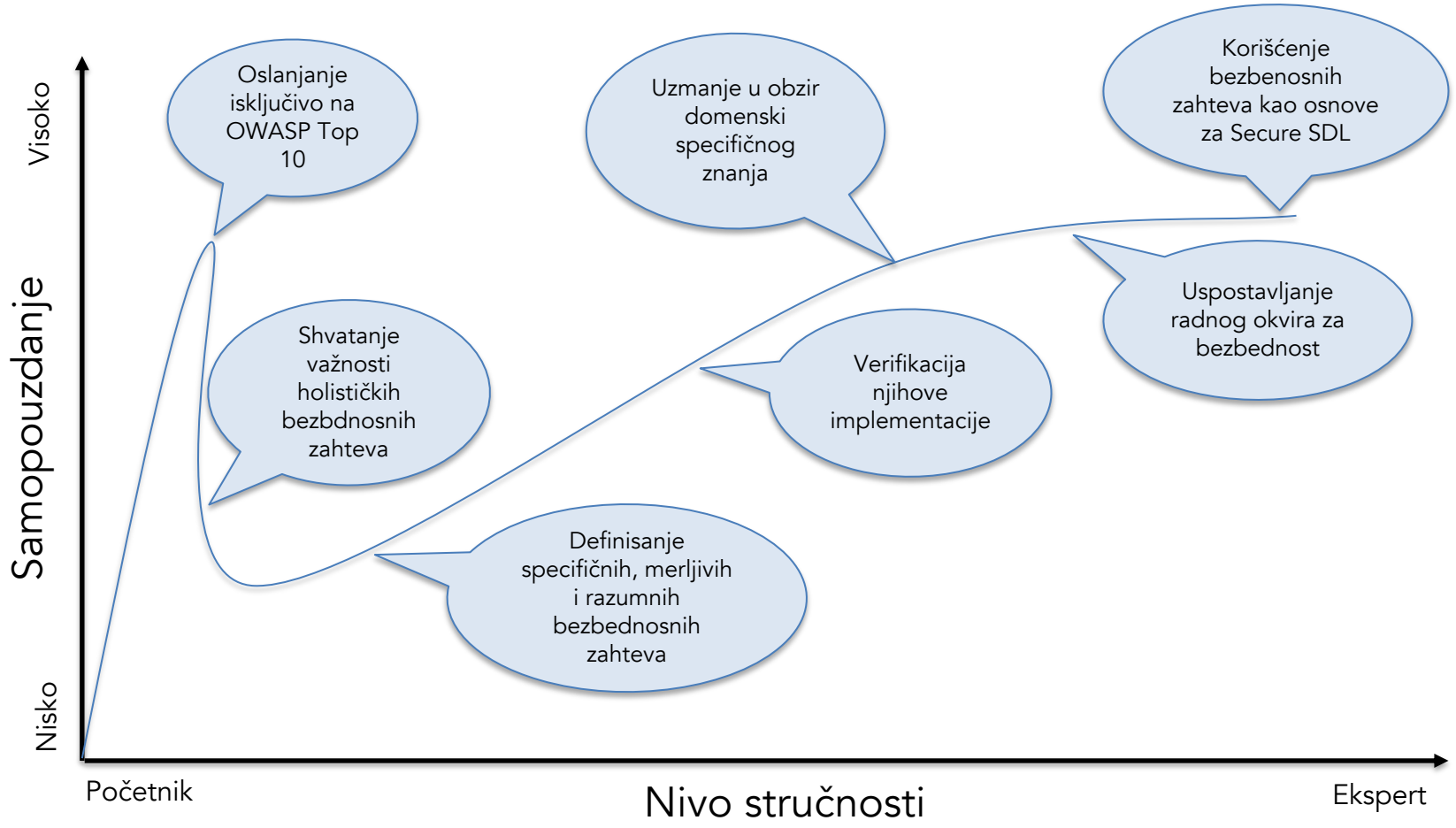
Pravljenje profila



Odlučivanje o resursima i budžetu

Potkategorija	Prioritet	Praznine (engl. gaps)	Budžet	Aktivnosti (godina 1)	Aktivnosti (godina 2)
1	Umeren	Mali	$$$		X
2	Visok	Veliki	$$	X	
3	Umeren	Srednji	$	X	
…	…	…	…		
98	Umeren	-	$$		ponovna procena

Dunning-Kruger efekat u inženjerstvu bezbednosnih zatheva



Dunning-Kruger efekat u inženjerstvu bezbednosnih zahteva
https://sec-consult.com/blog/detail/security-requirements-engineering-the-backbone-of-your-ssdlc/

Zaključak

- Bezbednosni zahtevi uspostavljaju osnovne mere neophodne za zaštitu osetljivih informacija, ublažavanje rizika i zaštitu sredstava organizacije od pretnji
- Poštovanje bezbednosnih zahteva obezbeđuje usklađenost sa propisima, smanjujući verovatnoću kazni, novčanih kazni i zakonskih obaveza povezanih sa nepoštovanjem
- Definisanjem specifičnih bezbednosnih mera, organizacije mogu efikasno da identifikuju, procene i ublaže rizike sajber bezbednosti, jačajući otpornost na potencijalne pretnje i ranjivosti
- Implementacija robusnih bezbednosnih zahteva doprinosi održavanju kontinuiteta poslovanja, minimizujući poremećaje i obezbeđujući neprekidnu isporuku proizvoda i usluga kupcima
- Ispunjavanje bezbednosnih zahteva podstiče poverenje među zainteresovanim stranama, uključujući kupce, partnere i investitore, demonstrirajući posvećenost zaštiti poverljivih informacija i održavanju integriteta poslovnih operacija

Dodatne Reference

- Tarandach I., J. Coles M. J. Threat Modeling – A Practical Guide for Development Teams. O'Reilly 2021.
- NIST Cybersecurity Framework (CSF) - https://www.nist.gov/cyberframework