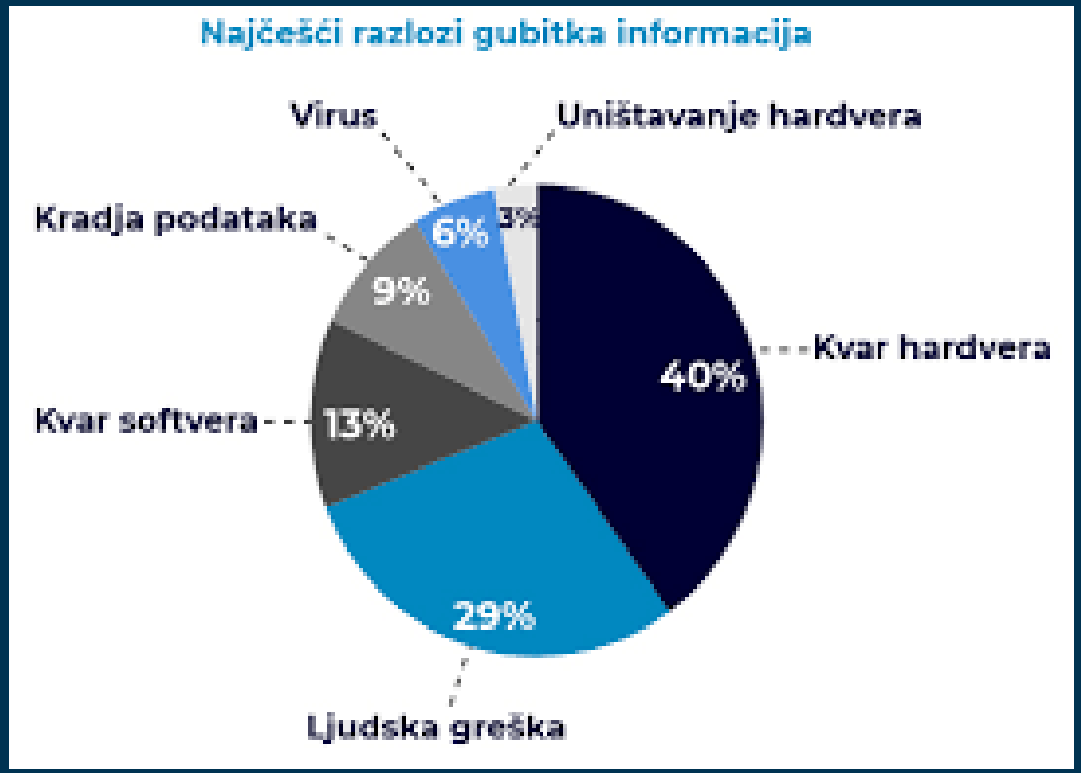
Bezbednost informacionih sistema

- Zakonski okvir, standardi i mehanizmi -

Da li ste znali?

- Šanse za oporavak kompanije, nakon značajnog gubitka poslovnih podataka usled katastrofe, su veoma male:
  - samo 6% se oporavi,
  - 43% ne nastavi da radi, a
  - 29% se zatvori u prve dve godine.

- Kompanije su izložene različitim rizicima koji mogu ozbiljno ugroziti njihovo poslovanje.
- Rizici su najčešće posledica otkaza hardvera, uticaja ljudskog faktora, grešaka u softveru, neovlašćenih upada u sistem, virusa, itd..
- Kao odgovor na navedene izazove, neophodno je preventivno planiranje i preduzimanje koraka u cilju obezbeđivanja poslovanja u slučaju neželjenog događaja.



- https://coming.rs/bezbednost/izrada-plana-za-kontinuitet-poslovanja/

Osnovni koncepti informacione bezbednosti

Bezbednost informacionog sistema obuhvata sve mere i aktivnosti koje imaju za cilj da zaštite podatke, aplikacije, mreže i infrastrukturu od neovlašćenog pristupa, zloupotrebe, gubitka i narušavanja integriteta podataka.

Zasniva se na tri osnovna principa poznata kao CIA trijada:

- **Poverljivost** (*Confidentiality*) – sprečavanje neovlašćenog pristupa informacijama;
- **Integritet** (*Integrity*) – očuvanje tačnosti i potpunosti podataka;
- **Dostupnost** (*Availability*) – obezbeđivanje da informacije i sistemi budu dostupni kada su potrebni;

Cilj je da se obezbedi stabilan, otporan i usklađen IT koji podržava poslovanje i štiti interese organizacije.

Dodatni koncepti u proširenim modelima

- **Privatnost** (*Privacy*) – posebno nagašena u kontekstu GDPR и ISO/IEC 27701
- **Otpornost** (*Resilience*) – sposobnost sistema da se oporavi od incidenata
- **Odgovornost** (*Accountability*) – praćenje i evidencija aktivnosti radi utvrđivanja odgovornosti

Zakonski okvir

Postavlja kontekst i obaveze

1. Zakon o informacionoj bezbednosti

- Osnovni zakon koji definiše mere zaštite IKT sistema, uloge operatera i nadležnih organa.
- Uvodi obavezu procene rizika, donošenje akta o bezbednosti i postupanju u slučaju incidenata.
- Utvrđuje ulogu Nacionalnog CERT-a i CERT-a organa vlasti.
- Obuhvata i IKT sisteme od posebnog značaja.
- U toku je usvajanje novog Zakona o informacionoj bezbednosti koji donosi brojne novine u skladu sa direktivom NIS2.

*CERT (енг. *Computer Emergency Response Team*)

Bezbednost IKT sistema (NIS)

- **NIS1** (Direktiva o sajber bezbednosti (EU) 2016/1148) je zakonodavni akt Evropskog parlamenta čiji je cilj bio da podigne nivo sajber bezbednosti širom Unije tako što će obezbediti primenu strogih mera bezbednosti u ključnim sektorima, kao što su: energetika, transport, bankarstvo, finansije, zdravstvo, voda i digitalna infrastruktura.

- NIS1 je zahtevao od država članica da razviju nacionalne strategije za sajber bezbednost, uspostave timove za reagovanje na incidente u računarskoj bezbednosti (CSIRT) i uvedu procedure upravljanja rizikom.

- **NIS2** (Direktiva o sajber bezbednosti (EU) 2022/2555) je zakonodavni akt Evropskog parlamenta koji menja prethodnu NIS1 direktivu i ima za cilj postizanje visokog zajedničkog nivoa sajber bezbednosti širom Unije.

*NIS (eng. *Network Information Security*)

Tim za reagovanje na incidente (CSIRT)

- **CSIRT** (eng. *Computer Security Incident Response Team*) je stručni tim za bezbednost IKT infrastrukture, koji reaguje na incidente u vezi sa sajber bezbednošću, fokusirajući se na suzbijanje štete, oporavak sistema i sprečavanje budućih napada.

- Često se naziva i **CERT** (eng. *Computer Emergency Response Team*), a njihova uloga uključuje analizu pretnji, koordinaciju odgovora na incidente, pružanje tehničke pomoći i obaveštavanje o bezbednosnim najboljim praksama i trendovima.

2. Zakon o zaštiti podataka o ličnosti

- Usklađen sa Zakonom o zaštiti podataka o ličnosti (GDPR), reguliše obradu ličnih podataka i prava pojedinca.
- Zahteva tehničke i organizacione mere zaštite podataka.
- Uvodi obavezu imenovanja lica za zaštitu podataka u određenim slučajevima.

*GDPR (eng. *General Data Regulation Protection*).

3. Zakon o elektronskim komunikacijama

- Uređuje bezbednost i integritet elektronskih komunikacionih mreža i usluga.
- Operateri treba da preuzmu mere zaštite i zloupotrebe od incidenata.
- Povezan sa NIS2 direktivom u kontekstu kritične infrastrukture.

Međunarodni standardi

Okvir za izgradnju sisgurnog IT okruženja

1. ISO/IEC 27001:2022

Bezbednost informacija, sajber bezbednost i zaštita privatnosti

- Sistemi menadžmenta bezbednošću informacija - Zahtevi

- Osnovni standard koji definiše zahteve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje ISMS-a.
- Omogućava organizacijama da sistematski upravljaju rizicima i demonstriraju usklađenost sa regulativama.
- Sertifikacija po ovom standardu je međunarodno priznata.

*ISMS (eng. *Information Security Management System*)

2. ISO/IEC 27002:2022

Bezbednost informacija, sajber bezbednost i zaštita privatnosti

- Kontrole bezbednosti informacija

- Pruža detaljne preporuke za primenu kontrolnih mera iz Aneksa A standarda ISO 27001.
- Obuhvata tehničke, fizičke i organizacione kontrole.
- Koristi se kao praktičan vodič za implementaciju bezbednosnih politika.

3. ISO/IEC 27031:2025

Spremnost informacionih i komunikacionih tehnologija za kontinuitet poslovanja

- Specijalizovan standard koji se bavi sposobnošću IKT sistema da podrže kontinuitet poslovanja.
- Uvodi koncepte planiranja, prevencije, otkrivanja, reagovanja i oporavka IKT usluga.
- Pokriva interne i eksterne zavisnosti i usklađen je sa ISO 22301 i ISO/IEC 27001.
- Omogućava organizacijama da definišu parametre za oporavak IKT resursa i referentna vremena:
  - **RTO** – Vreme oporavka sistema (*Recovery Time Objective*),
  - **RPO** – Tolerisani gubitak podataka (*Recovery Point Objective*), i
  - **MAO** – Maksimalno dozvoljeni prekid rada (*Maximum Allowable Outage*).

4. ISO 22301:2020

Bezbednost i otpornost – Sistemi menadžmenta kontinuitetom poslovanja - Zahtevi

- Predstavlja međunarodni standard za uspostavljanje, implementaciju i održavanje sistema upravljanja kontinuitetom poslovanja.
- Fokusira se na identifikaciju kritičnih funkcija, procenu uticaja prekida (eng. *Business Impact Analysis* – BIA) i definisanje strategija oporavka.
- Ključan za organizacije koje žele da obezbede otpornost i brz oporavak nakon incidenata, katastrofa ili tehničkih kvarova.

Postupanje sa rizicima (*Risk treatment*)

Postupanje sa rizikom obuhvata sve aktivnosti koje imaju za cilj modifikovanje rizika, što uključuje:

- **Izbegavanje rizika** (*risk avoidance*) – donošenje odluke da se ne preduzimaju korektivne akcije,
- **Prihvatanje rizika** (*risk acceptance*) – svesno zadržavanje rizika bez dodatnih mera,
- **Ublažavanje rizika** (*risk mitigation*) – sprovođenje preventivnih mera u cilju smanjenja rizika,
- **Transfer rizika** (*risk transference*) - prenos rizika na treću stranu (npr. osiguranje, outsourcing), i
- **Odvraćanje od rizika** (*risk deterrence*) – podrazumeva kaznene mere protiv potencijalnih neprijatelja.

Zaštita informacija u praksi

Praktična primena bezbedonosnih alata i procedura

Organizacione i procesne mere

Politika bezbednosti informacija

Obuka zaposlenih

Procena rizika i klasifikacija podataka

Rezervne kopije i oporavak

(Backup & Recovery)

Planiranje kontinuiteta poslovanja (BCP) i oporavak od katastrofe (DRP)

Politike bezbednosti informacija: formalno definisana pravila i smernice kojima se reguliše način zaštite podataka, odgovornosti zaposlenih i postupanje u slučaju bezbednosnih incidenata. Pokriva interne i eksterne zavisnosti i usklađene su sa ISO 22301 i ISO/IEC 27001.

Obuka zaposlenih: podiže se svest o rizicima, unapređuje bezbednosna kultura i obezbeđuje pravilno postupanje u skladu sa politikom zaštite podataka.

Procena rizika i klasifikacija podataka: omogućavaju organizaciji da identifikuje kritične informacije, proceni potencijalne pretnje i primeni odgovarajuće mere zaštite u skladu sa značajem i osetljivošću podataka.

Rezervne kopije i oporavak: ključne mere za očuvanje dostupnosti i integriteta podataka. Omogućavaju organizaciji da se brzo vrati u normalan rad nakon tehničkih kvarova, incidenata ili katastrofa

Planiranje kontinuiteta poslovanja (BCP) i oporavka od katastrofe (DRP): strukturiran pristup očuvanju kritičnih funkcija i brzom tehničkom oporavku. Obezbeđuju otpornost organizacije u slučaju prekida, havarija ili sajber incidenata.

Tehničke mere zaštite (1)

Zaštitni zid sledeće generacije

Next-Generation Firewall

Segmentacija mreže

Detekcija pretnji sledeće generacije

Next-Generation Threat Detection

Kontrola pristupa

SIEM/SOAR i sistem za otkrivanje ranjivosti

Zaštitni zid sledeće generacije (Next-Generation Firewall): omogućava dubinsku analizu saobraćaja, prepoznavanje aplikacija i korisnika, kao i proaktivnu zaštitu od pretnji uz primenu mehanizama kao što su DPI, sandboxing i integracija sa sistemima zaštite krajnjih tačaka.

Segmentacija mreže: tehnička mera kojom se mrežna infrastruktura deli na logičke ili fizičke zone, čime se smanjuje površina napada, ograničava kretanje pretnji i omogućava preciznija kontrola pristupa među sistemima.

Antivirusni sistem sledeće generacije: napredni bezbednosni sistem koji omogućava kontinuirano praćenje, otkrivanje i reagovanje na pretnje na krajnjim uređajima, uz mogućnost forenzičke analize, izolacije uređaja i automatizovanog otklanjanja incidenata.

Kontrola pristupa: skup tehničkih i organizacionih mera kojima se reguliše ko, kada i pod kojim uslovima može da pristupi određenim informacijama, sistemima ili resursima.

SIEM/SOAR sistemi: napredna platforma za upravljanje bezbednosnim informacijama i odgovorom na incidente, gde SIEM omogućava prikupljanje, korelaciju i analizu bezbednosnih događaja, a SOAR automatizuje reagovanje, orkestraciju i dokumentaciju incidenata.

Sistem za otkrivanje ranjivosti: omogućava identifikaciju bezbednosnih slabosti u IT infrastrukturi, pre nego što budu iskorišćene u napadu.

*SIEM (eng. *Security Information and Event Management*)

*SOAR (eng. *Security Orchestration, Automation, and Response*)

*DPI (eng. *Deep Packet Inspection*)

Tehničke mere zaštite (2)

Zaštitni zid Web aplikacija

Web Application Firewall (WAF)

Zaštita elektronske pošte

Kriptografska zaštita

Upravljanje pečevima

(Patch Management)

Bezbednosna konfiguracija sistema

WAF - Web Application Firewall: Štiti web aplikacije od napada filtriranjem, nadzorom i blokiranjem zlonamernog HTTP saobraćaja.

Zaštita elektronske pošte: Sprečava phishing, spam i malver kroz filtriranje sadržaja, autentifikaciju pošiljalaca i šifrovanje poruka.

Kriptografska zaštita: Obezbeđuje poverljivost i integritet podataka korišćenjem šifrovanja, digitalnih potpisa i sigurnih protokola.

Upravljanje pečevima: Redovno ažuriranje softvera radi uklanjanja poznatih ranjivosti i sprečavanja iskorišćavanja sigurnosnih propusta.

Bezbednosna konfiguracija sistema: Hardening sistema kroz onemogućavanje nepotrebnih servisa, primenu sigurnosnih politika i kontrolu pristupa.

Kontinuitet poslovanja IKT sistema

Analiza uticaja na poslovanje i procena rizika u IKT sistemima

Plan kontinuiteta poslovanja IKT sistema

(BC plan)

Plan odgovoira na incidente u IKT sistemu

(IR plan)

Plan oporavka IKT sistema u slučaju krizne situacije

(DR plan)

Plan oporavka poslovanja Službe za IT

(BR plan)

Analiza uticaja na poslovanje za IKT sisteme (BIA analiza) i procena rizika sa matricom uticaja: Dokument predstavlja strukturiranu procenu kritičnih IKT funkcija kroz BIA analizu i procenu rizika, uz primenu matrice uticaja radi definisanja prioriteta oporavka i mera zaštite.

Plan kontinuiteta poslovanja IKT sistema (BC plan): definiše strukturu, procedure i resurse neophodne za očuvanje kritičnih IKT funkcija Službe za IT u slučaju prekida, uz utvrđene scenarije, vremenske okvire oporavka i odgovornosti.

Plan odgovora na incidente u IKT sistemu (IR plan): opisuje procedure, uloge i komunikacione tokove za blagovremenu identifikaciju, eskalaciju i rešavanje IKT incidenata, uz definisane faze reakcije, alate za evidenciju i kriterijume za aktiviranje tima za odgovor na incidente.

Plan oporavka IKT sistema u slučaju krizne situacije (DR plan): opisuje tehničke i organizacione mere za vraćanje IKT sistema u operativno stanje nakon krizne situacije, uključujući scenarije havarija, vremenske okvire oporavka, rezervne resurse i procedure za aktiviranje DR infrastrukture.

Plan oporavka poslovanja Službe za IKT (BR plan): definiše korake, resurse i odgovornosti neophodne za obnovu poslovnih funkcija Službe za informacione tehnologije nakon prekida, uz integraciju tehničkih i organizacionih mera, vremenskih okvira i scenarija za vraćanje svih IKT usluga u operativno stanje — pri čemu se ne predviđa aktiviranje DR lokacije, već se oporavak sprovodi u primarnom okruženju.

Hvala na pažnji.