Univerzitet Donja Gorica
ERASMUS+ Projekat „CSupMNE“
Broj: 12/25
Podgorica, 03.11.2025

KONZORCIJUM UNIVERZITETA: Univerzitet Donja Gorica, Univerzitet Crne Gore, Univerzitet Mediteran i Univerzitet Adriatik

Vas pozivaju da uzmete učešće u procesu dostavljanja ponuda za izbor najpovoljnijeg dobavljača za izradu softvera i nabavku hardvera za potrebe realizacije ERASMUS + projekta
ERASMUS-EDU-2024-CBHE-STRAND-3/ERASMUS2027/101179688
„Straightening Up Cybersecurity Posture of Montenegrin Higher Education System“

I PREDMET NABAVKE:

Predmet nabavke je Usluga izrade Softvera i nabavka Hardvera neophodnog za:

1. **Procijenu, analizu i upravljanje sajber bezbjednostnim rizicima** na univerzitetetima Crne Gore
2. Podršku funkcionisanja **Nacionalnog akademskog CSIRT-a Crne Gore** (Computer Security Incident Response Team)

za potrebe realizacije ERASMUS + projekta ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688 „Straightening Up Cybersecurity Posture of Montenegrin Higher Education System“ prema specifikaciji:

Lot 1. Izradu softvera za Procijenu, analizu i upravljanje sajber bezbjednostnim rizicima na univerzitetetima Crne Gore.

1. Izradu softvera za Procijenu, analizu i upravljanje sajber bezbjednostnim rizicima na univerzitetetima Crne Gore			
R. br	**Modul**	**Opis**	**Količina**
1.	Modul I: Identifikacija rizika:	Ovaj modul omogućava sveobuhvatnu identifikaciju digitalnih resursa (informacija, sistema, servisa), prijetnji (npr. malware, phishing, neovlašćeni pristup) i ranjivosti u okruženju visokoobrazovnih institucija. Ova funkcija je podržana interaktivnim vodičima i bazama prijetnji relevantnim za akademski sektor.	1

2.	Modul II: Procjena i analiza rizika	Ovaj modul omogućava kvalitativnu i kvantitativnu procjena rizika, uz upotrebu matrica rizika koje se mogu prilagoditi specifičnostima univerziteta. Alat pomaže korisnicima da razumiju vjerovatnoću realizacije prijetnji i potencijalne posljedice po ključne funkcije i informacije.	1
3.	Modul III: Upravljanje i tretman rizika	Ovaj modul omogućava korisnicima da na osnovu rezultata analize, mogu definisati strategije tretmana rizika (izbjegavanje, smanjenje, transfer, prihvatanje) i povezati ih sa konkretnim tehničkim, organizacionim i proceduralnim mjerama zaštite.	1
4.	Modul IV: Praćenje i revizija	Ovaj modul omogućava kontinuirano praćenje identifikovanih rizika, statusa primijenjenih mjera, kao i automatsko generisanje obavještenja u slučaju promjena u profilu rizika. Takođe, podržava reviziju i ponovno vrednovanje rizika u skladu sa promjenama u okruženju i zakonodavstvu.	1
5.	Modul V: Izvještavanje i transparentnost	Ovaj modul omogućava automatsko kreiranje detaljnih i sumiranih izvještaja za različite nivoe upravljanja – od IT timova do rukovodstva univerziteta i regulatornih tijela. Izvještaji su prilagođeni zahtjevima nacionalnih i međunarodnih standarda i uključuju sve ključne indikatore performansi u oblasti sajber bezbjednosti	1
6.	Modul VI: Višenivojski pristup i decentralizovana upotreba	Ovaj modul omogućava upotrebu na različitim organizacionim nivoima univerziteta – rektorat, fakulteti, instituti, IT službe – uz jasno definisane uloge i ovlašćenja korisnika, čime se podržava decentralizovano, ali usklađeno upravljanje rizicima	1
7.	Modul VII: Lokalizacija i usklađenost sa crnogorskim okvirom	Ovaj modul omogućava lokalizaciju na crnogorski jezik, uz podršku za pravne i institucionalne specifičnosti visokog obrazovanja u Crnoj Gori. Usklađen je sa domaćim zakonodavstvom i politikama, uključujući Zakon o informacionoj bezbjednosti, Strategiju sajber bezbjednosti	1

		Crne Gore i preporuke Ministarstva prosvjete, nauke i inovacija.	
8.	Modul VIII - Integracija sa Nacionalnim akademskim CSIRT-om	Ovaj modul omogućava integraciju sa uslugama budućeg Nacionalnog akademskog CSIRT tima, omogućavajući dvosmjernu razmjenu informacija o incidentima, preporukama za sanaciju i unapređenje preventivnih mjera.	1

Procijenjena vrijednost nabavke je 50.000,00€ bez PDV.

Lot 2. Izrada Softvera za podršku radu Nacionalnog akademskog CSIRT-a Crne Gore (Computer Security Incident Response Team) i nabavka Hardvera

2. Izrada Softvera za podršku radu Nacionalnog akademskog CSIRT-a Crne Gore (Computer Security Incident Response Team).			
R. br	**Modul**	**Opis**	**Količina**
1.	Modul I: Informacioni bezbjednosni događaji (Information Security Event Management).	Ovaj modul predstavlja osnovu za rano otkrivanje potencijalnih incidenata kroz analizu podataka prikupljenih kontinuiranim nadzorom informacionih sistema. Glavni cilj je omogućiti CSIRT timu i organizaciji da pravovremeno identifikuju anomalije i potencijalne prijetnje, smanjujući rizik od ozbiljnijih incidenata. Modul obuhvata ključni servis i funkciju: Prihvatanje događaja za analizu sa kvalifikacijom događaja radi razlikovanja stvarnih incidenata od lažnih alarma.	1
2.	Modul II: Upravljanje incidentima (Information Security Incident Management)	Cilj ovog modula je da obezbedi efikasnu obradu, analizu i koordinaciju u slučaju sigurnosnih incidenata, omogućavajući organizacijama da brzo reaguju i minimiziraju posledice. Servisi uključuju prijem i potvrdu prijava incidenata, triage i inicijalnu obradu prijava kako bi se identifikovali prioriteti, i analizu incidenata koja obuhvata kategorizaciju, prioritetizaciju, prikupljanje dokaza i korelaciju incidenata. Funkcije podrške za mitigaciju i oporavka omogućavaju planiranje odgovora, ad-hoc mere kao i podrška za povraćaj sistema i podataka. Osnovna funkcija Modula je koordinacija i komunikacija, uključujući interne i eksterne kanale (TLP), generisanje notifikacija i izveštaja, medijsku komunikaciju, kao i podršku kriznom menadžmentu kroz distribuciju statusa i strateških odluka. Softverski zahtevi uključuje modul za lifecycle incidenata, portal za prijave incidenata i automatizovana izvještavanja koja omogućavaju brzo donošenje odluka i transparentnost procesa.	1

| **PROJECT COORDINATOR:** University of Donja
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

3.	Modul III: Upravljanje ranjivostima (Vulnerability Management).	Ovaj modul je fokusiran na prihvatanje prijava za isporuku servisa analize i odgovor na ranjivosti u informacionim sistemima, čime se smanjuje površina za potencijalne napade. Servis uključuje koordinaciju sa vendorima i partnerima, kao i objavljivanje i distribuciju saveta za ranjivosti (vulnerability disclosure) kako bi se zajednica obavestila o prijetnjama i preporučenim merama. Odgovor na ranjivosti uključuje korišćenje skenera, remedijaciju i patch management, čime se efikasno zatvaraju sigurnosni propusti.	1
4.	Modul IV: Situaciona svest (Situational Awareness)	Situaciona svest (Situational Awareness). Cilj ovog modula je proaktivno razumevanje pretnji i pružanje informacija akademskoj zajednici i korisnicima sistema kako bi se povećala spremnost i smanjio rizik od incidenata. Servisi obuhvataju prikupljanje podataka kroz policy mapping, asset mapping i integraciju sa threat intelligence feedovima, analizu i sintezu podataka radi identifikacije trendova incidenata i pružanja podrške u odlučivanju, kao i komunikaciju kroz izveštaje, preporuke i razmenu informacija sa ključnim akterima.	1
5.	Modul V: Transfer znanja (Knowledge Transfer).	Ovaj modul ima za cilj edukaciju, podizanje svesti i jačanje kapaciteta korisnika i članova organizacije. Servisi uključuju podizanje svesti kroz kampanje, newsletter-e i izveštaje o pretnjama, obuku i edukaciju kroz kurseve, e-learning platforme i mentoring programe, kao i savjetodavne usluge vezane za upravljanje rizicima i podršku u kreiranju politika. Softverski zahtevi uključuju e-learning modul, repozitorijum znanja i alat za generisanje izveštaja, čime se omogućava kontinuirana edukacija, povećava otpornost organizacije i jačaju veštine u upravljanju incidentima.	1

3. Nabavka Hardverske platforme za predložena softverska rješenja: 1. Za Procijenu, analizu i upravljanje sajber bezbjednostnim rizicima na univerzitetetima Crne Gore i 2. Softvera za podršku radu Nacionalnog akademskog CSIRT-a Crne Gore (Computer Security Incident Response Team).

5.	Aplikativni Server	Tehničke karakteristike uređaja trebaju obezbjediti sigurnu, kontinuiranu i efikasnu funkcionalnost softverske pltaforme	1
6.	Server baze podataka		1
7.	Firewall zaštita		1
8.	Backup uređaj		1
3. Nabavka Sistemskog softvera za Softversku i Hardversku Plaformu			
9.	Serverski Operativni sistem	Karakteristike sistemskog softevra trebaju obezbjediti sigurnu, kontinuiranu i efikasnu funkcionalnost softverske pltaforme	1
10.	Sistem upravljanja bazom podataka		1
11.	Server Antivirus		1
4. Tehničko održavanje Softverske i Hardverske platforme			
12.	Tehničko održavanje	Tehničko održavanje softverske i hardverske platforme u trajanju od 2 godine	1

Procijenjena vrijednost nabavke je 50.000,00€ bez PDV.

II Ponuda treba da sadrži:

1 Opšti dio:

- Idejno rješenje Softverske platforme sa opisom funkcionalnosti za navedene module.
- Detaljnu tehničku specifikaciju Hardverske platforme i predloženog sistemskog softvera
- Tačan naziv i adresu ponuđača, poreski i identifikacioni broj;
- Kontakt ovlašćenog predstavnika sa neograničenim pregovaračkim ovlašćenjem u vezi predmeta nabavke;
- Reference ponuđača da je učestvovao u implementaciji softverskog rešenja vezano za Upravljanje sajber bezbjednostnim rizicima i da je učestvovao u nabavci hardvera i sistemskog softvera za potrebe Erasmsus+ projekta;
- Garantni rok na isporučenu robu;
- Digitalna i papirna forma ponude (original + 2 kopije).

2 Komercijalni dio:

- Ponudu dati u jediničnim cijenama, sa i bez PDV-a;
- Ukupna vrijednost ponude izražene u €, sa i bez PDV-a;
- Naznačiti dinamiku i način plaćanja.

III Minimum zahtjeva koje ponuda mora da ispuni:

- Da idejna rješenja obuhvataju sve navedene module u skladu sa zahtjevima definisanim u tehničkim uslovima;
- Da ponuđač ima minimum jedno softversko rješenje u oblasti upravljanja sajber bezbjednostnim rizicima i da je izvršio nabavku hardvera i sistemskog softvera za minimum jedan Erasmsus+ projekat;

| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

- Prihvatanje uslova plaćanja minimum 30 dana od datuma isporuke sotfvera-licenci i izdavanja komercijalne fakture;
- Ponuda mora biti obavezujuća na period od 60 dana. Konzorcijum Univerzitet, zadržava pravo na mogućnost produženje ovog roka.

IV Uslovi izvršavanja:
U slučaju da izabrani ponuđač odustane od izvršenja ugovora, ili obaveze izvršava suprotno ugovorenom, Konzorcijum univerziteta se može obratiti drugo rangiranom ponuđaču radi zaključivanja ugovora.

V Kriterijumi vrednovanja ponuda:
Da bi ponuda mogla biti razmatrana mora ispuniti uslove iz opšteg dijela ponude; komercijalnog dijela ponude i mora zodovoljiti minimalne zahtjeve definisane u poglavlju III. Ponude koje ne zadovolje gore pomenute uslove neće biti razmatrane.

Vrednovanje ponuda u ukupnom iznosu od 100 poena obavlja se na sledeći način:

- Kvalitet Idejnog rješenja softverske platforme ……. 50 poena
- Cijena ……..….. 50 poena

VI Dostavljanje ponuda:
Obavezno je opšti i komercijalni dio ponude dostaviti u posebnim i zapečaćenim kovertama sa naznakom na koverti da li se radi o opštem ili komercijalnom dijelu ponude.

Obje koverte dostaviti u trećoj zapečaćenoj koverti na arhivu Univerziteta Donja Gorica Podgorica (ul. Oktoih 1) radnim danima od 09.00-16.00h, sa naznakom:

Za tender nabavku usluga izrade Softvera i nabavka Hardvera neophodnog za potrebe ERASMUS+ projekta "CSupMNE"– Ne otvarati osim u prisustvu tenderske komisije

Rok za dostavljanje ponuda je 12. 12. 2025. godine do 12.00h.

Kontakt osoba:
Prof.dr Ramo Šendelj
Tel: +382 67 226 333
E-mail: ramo.sendelj@udg.edu.me

Opis Tehničkih zahtjeva korisnika za

Izradu softvera za Procijenu, analizu i upravljanje sajber bezbjednostnim rizicima na univerzitetetima Crne Gore

za potrebe realizacije Erasmus + projekta
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
„Straightening Up Cybersecuirty Posture of Montenegrin Higheer Education System“

Uvodne napomene

Softver za procjenu, analizu i upravljanje sajber bezbjednosnim rizicima predstavlja ključni digitalni alat namijenjen univerzitetima u Crnoj Gori, razvijen s ciljem da podrži visokoobrazovne institucije u uspostavljanju sistematskog i održivog pristupa upravljanju sajber rizicima. U kontekstu sve češćih sajber prijetnji i rastuće digitalizacije obrazovnih i istraživačkih procesa, ovaj softver omogućava univerzitetima da na efikasan, strukturiran i transparentan način upravljaju rizicima koji ugrožavaju povjerljivost, integritet i dostupnost informacija, digitalne infrastrukture i servisa.

Glavni elementi softvera za procjenu, analizu i upravljanje sajber bezbjednosnim rizicima

Softver treba da bude u potpunosti usklađen sa međunarodnim standardima i najboljim praksama iz oblasti sajber bezbjednosti i upravljanja rizicima, uključujući ISO/IEC 27001 i 27005, NIST Cybersecurity Framework 2.0 i ENISA smjernice za sektor obrazovanja. Njegova arhitektura terba da bude modularna, sa sljedećim ključnim funkcionalnim modulima:

1. ***Modul - Identifikacija rizika:*** Ovaj modul omogućava sveobuhvatnu identifikaciju digitalnih resursa (informacija, sistema, servisa), prijetnji (npr. malware, phishing, neovlašćeni pristup) i ranjivosti u okruženju visokoobrazovnih institucija. Ova funkcija je podržana interaktivnim vodičima i bazama prijetnji relevantnim za akademski sektor.
2. ***Modul - Procjena i analiza rizika:*** Ovaj modul omogućava kvalitativnu i kvantitativnu procjena rizika, uz upotrebu matrica rizika koje se mogu prilagoditi specifičnostima univerziteta. Alat pomaže korisnicima da razumiju vjerovatnoću realizacije prijetnji i potencijalne posljedice po ključne funkcije i informacije.
3. ***Modul - Upravljanje i tretman rizika:*** Ovaj modul omogućava korisnicima da na osnovu rezultata analize, mogu definisati strategije tretmana rizika (izbjegavanje, smanjenje, transfer, prihvatanje) i povezati ih sa konkretnim tehničkim, organizacionim i proceduralnim mjerama zaštite.
4. ***Modul - Praćenje i revizija:*** Ovaj modul omogućava kontinuirano praćenje identifikovanih rizika, statusa primijenjenih mjera, kao i automatsko generisanje obavještenja u slučaju promjena u profilu rizika. Takođe, podržava reviziju i ponovno vrednovanje rizika u skladu sa promjenama u okruženju i zakonodavstvu.
5. ***Modul - Izvještavanje i transparentnost:*** Ovaj modul omogućava automatsko kreiranje detaljnih i sumiranih izvještaja za različite nivoe upravljanja – od IT timova do

rukovodstva univerziteta i regulatornih tijela. Izvještaji su prilagođeni zahtjevima nacionalnih i međunarodnih standarda i uključuju sve ključne indikatore performansi u oblasti sajber bezbjednosti.

6. ***Modul - Višenivojski pristup i decentralizovana upotreba:*** Ovaj modul omogućava upotrebu na različitim organizacionim nivoima univerziteta – rektorat, fakulteti, instituti, IT službe – uz jasno definisane uloge i ovlašćenja korisnika, čime se podržava decentralizovano, ali usklađeno upravljanje rizicima.
7. ***Modul - Lokalizacija i usklađenost sa crnogorskim okvirom:*** Ovaj modul omogućava lokalizaciju na crnogorski jezik, uz podršku za pravne i institucionalne specifičnosti visokog obrazovanja u Crnoj Gori. Usklađen je sa domaćim zakonodavstvom i politikama, uključujući Zakon o informacionoj bezbjednosti, Strategiju sajber bezbjednosti Crne Gore i preporuke Ministarstva prosvjete, nauke i inovacija.
8. ***Modul - Integracija sa Nacionalnim akademskim CSIRT-om:*** Ovaj modul omogućava integraciju sa uslugama budućeg Nacionalnog akademskog CSIRT tima, omogućavajući dvosmjernu razmjenu informacija o incidentima, preporukama za sanaciju i unapređenje preventivnih mjera.

Primjenom ovog softvera, univerziteti u Crnoj Gori će značajno unaprijediti svoju sposobnost da identifikuju, razumiju i kontrolišu sajber rizike, čime se podiže nivo ukupne bezbjednosti obrazovno-istraživačkog sektora. Softver takođe doprinosi jačanju bezbjednosne kulture, podizanju svijesti i stvaranju održivih institucionalnih kapaciteta za sajber otpornost u skladu sa savremenim izazovima digitalnog društva.

1. DETALJNI PRIKAZ MODULA

1. Modul I „Identifikacija rizika”

Modul predstavlja prvu i jednu od najvažnijih faza u procesu upravljanja sajber bezbjednosnim rizicima. Ovaj modul omogućava univerzitetima i njihovim organizacionim jedinicama da na sistematičan, sveobuhvatan i ponovljiv način identifikuju ključne informacione resurse, prijetnje kojima su izloženi i ranjivosti koje mogu biti iskorišćene, kao osnovu za dalju procjenu, analizu i tretman rizika.

Ključne funkcionalnosti modula:

1.1. Mapiranje informacionih resursa

- Omogućava korisnicima da identifikuju i katalogizuju sve relevantne informacione resurse:
    - *Tehnički resursi*: serveri, mrežna oprema, računari, softveri, baze podataka.
    - *Informacioni sistemi i aplikacije:* IS za studentske usluge, eLearning platforme, sistemi za upravljanje naučnim istraživanjima itd.
    - *Podaci:* lični podaci studenata i zaposlenih, istraživački podaci, povjerljive informacije.

- *Ljudski resursi:* ključni zaposleni sa pristupom kritičnim sistemima.
- Podržava klasifikaciju resursa prema važnosti, kritičnosti, vlasništvu i funkcionalnoj ulozi, u skladu sa politikama informacionog upravljanja.

1.2. Identifikacija prijetnji

- Softver pruža ugrađenu bazu tipičnih sajber prijetnji relevantnih za visoko obrazovanje, koja uključuje:
  - Malware napade (ransomware, spyware)
  - Phishing i socijalni inženjering
  - Neovlašćeni pristup i curenje podataka
  - Sabotažu od strane zaposlenih
  - Tehničke kvarove i greške u konfiguraciji
  - Napade na dostupnost (DDoS)
- Korisnici mogu dodatno unositi lokalne ili specifične prijetnje identifikovane internim analizama ili putem Nacionalnog akademskog CSIRT-a.

1.3. Identifikacija ranjivosti

- Sistem omogućava unos i ažuriranje informacija o poznatim ranjivostima:
  - Nedovoljno zaštićeni sistemi
  - Zastarjeli softver i operativni sistemi
  - Loše postavljene kontrole pristupa
  - Nedostatak obuke kod osoblja
  - Neadekvatne sigurnosne kopije (backup)
- Moguća je integracija sa alatima za automatsko skeniranje ranjivosti ili ručni unos na osnovu internog IT pregleda.

1.4. Povezivanje prijetnji, ranjivosti i resursa

- Sistem koristi relacione mape koje vizuelno prikazuju odnos između resursa, prijetnji i ranjivosti.
- Na primjer: studentski informacioni sistem → koristi Apache server → ranjiv na CVE-2024-xxxx → podložan DDoS napadima i curenju podataka.
- Ova funkcionalnost omogućava sveobuhvatno razumijevanje potencijalnih scenarija rizika.

1.5. Standardizovani opisi i katalozi

- Softver koristi unaprijed definisane kataloške liste resursa, prijetnji i ranjivosti u skladu sa standardima:
  - ENISA Threat Landscape
  - NIST SP 800-30 / 800-53
  - ISO/IEC 27005 i ISO/IEC 27002

1.6. Podrška za saradnički unos i validaciju podataka

- Višekorisnički interfejs omogućava IT osoblju, menadžerima, nastavnom osoblju i CSIRT timovima da unose podatke u okviru svojih nadležnosti.
- Postoji sistem za reviziju i odobravanje unosa, čime se obezbjeđuje tačnost i dosljednost.

1. 7. Generisanje izveštaja o identifikovanim rizicima

- Modul automatski kreira izvještaje koji sadrže:
  - Listu svih identifikovanih informacija i sistema
  - Povezane prijetnje i ranjivosti
  - Početni (neocijenjeni) nivo potencijalnog rizika
- Izvještaji se mogu izvesti u PDF/Excel formatima i koristiti u daljoj fazi procjene i odlučivanja.

2. Modul II „Procjena i analiza rizika”

Modul je centralna komponenta softverskog sistema za upravljanje sajber bezbjednosnim rizicima na univerzitetima u Crnoj Gori. Ovaj modul omogućava strukturiranu, objektivnu i ponovljivu evaluaciju nivoa rizika po informacione resurse i sisteme, na osnovu prethodno identifikovanih prijetnji, ranjivosti i važnosti resursa. Njegova svrha je da podrži donošenje informisanih odluka o prioritetima u zaštiti, alokaciji resursa i planiranju odgovora na bezbjednosne izazove.

Glavne funkcionalnosti modula:

2.1. Definisanje metodologije procjene rizika

- Modul omogućava izbor ili definisanje metodologije procjene rizika u skladu sa međunarodnim standardima (ISO/IEC 27005, NIST SP 800-30, CRAMM i dr.).
- Univerzitet može koristiti:
  - ***Kvalitativnu procjenu*** (npr. skaliranje rizika: nizak, srednji, visok)
  - ***Kvantitativnu procjenu*** (izraženu u brojčanom obliku, npr. monetarna vrijednost štete)
  - ***Hibridni pristup*** (kvalitativni pokazatelji sa brojčanim težinama)

2.2. Procjena vjerovatnoće i uticaja

- Sistem omogućava procjenu svakog identifikovanog rizika na osnovu dvije ključne dimenzije:
  - *Vjerovatnoća ostvarenja prijetnje (P)* – koliko je vjerovatno da će prijetnja biti realizovana uz prisustvo postojeće ranjivosti.
  - *Uticaj (I)* – kakve posljedice bi nastale po resurs, ako bi prijetnja bila ostvarena.
- Korisnici biraju vrijednosti iz unaprijed definisanih skala, koje mogu biti:
  - Skale od 1 do 5 (veoma niska do veoma visoka)
  - Opisi: npr. *rijetko*, *moguće*, *vjerovatno*, *gotovo izvjesno*
- Sistem automatski računa *početni rizik*: `Rizik = Vjerovatnoća × Uticaj`

2.3. Matrice rizika (Risk Matrix Generator)

- Modul uključuje generator vizuelnih matrica rizika (Risk Heatmaps) koje grafički prikazuju:
  - Lokaciju svakog rizika na osi vjerovatnoće i uticaja
  - Boje koje označavaju nivoe rizika: npr. zelena (nizak), žuta (srednji), crvena (visok)
- Matrice se mogu generisati:
  - Za pojedinačne organizacione jedinice
  - Za cijeli univerzitet
  - Za određene kategorije resursa (npr. podaci, sistemi, IT oprema)

2.4. Procjena postojećih kontrola (Control Evaluation)

- Sistem omogućava unos i analizu *postojećih bezbjednosnih mjera (kontrola)* koje utiču na nivo rizika:
  - Fizičke kontrole (npr. zaključane server sobe)
  - Tehničke kontrole (antivirus, firewall, šifrovanje)
  - Administrativne kontrole (politike, obuke, procedure)
- Korisnik unosi:
  - Tip kontrole
  - Stepen efikasnosti (npr. niska, srednja, visoka)
- Na osnovu ovoga, softver automatski računa *rezidualni (preostali) rizik*:
  `Rezidualni rizik = Početni rizik – Efikasnost kontrola`

2.5. Prioritizacija rizika

- Sistem automatski rangira rizike prema njihovom značaju (rezidualni nivo) I omogućava menadžmentu da identifikuje kritične tačke i „top 10” rizika koji zahtijevaju hitno djelovanje.
- Moguća sortiranja i filtriranja:
  - Po organizacionoj jedinici
  - Po vrsti resursa
  - Po nivou rizika

2. 6. Kontekstualizacija i atribucija rizika

Modul omogućava da se svakom riziku pridruže dodatni podaci I doprinosi transparentnosti i odgovornosti u upravljanju rizicima:

- Odgovorno lice ili služba
- Lokacija resursa
- Povezani propisi (npr. GDPR, Zakon o informacionoj bezbjednosti)
- Datum procjene i datum revizije

2.7. Praćenje promjena i istorijat procjena

- Sistem bilježi svaku promjenu i omogućava revizijski trag i analizu trenda (da li se rizik povećava ili smanjuje) u:
  - Procjeni vjerovatnoće i uticaja
  - Stanju postojećih kontrola
  - Pristupu tretiranju rizika

2.8. Izvještavanje i eksport podataka

- Generisanje izvještaja u više formata (PDF, Excel, Word) uključujući:
  - Liste rizika sa procjenom
  - Vizualizacije (grafikoni, heatmaps, top rizici)
  - Rezime po fakultetima, institutima ili projektima
- Moguće generisanje izvještaja za:
  - Internu upotrebu (menadžment, IT timove)
  - Eksternu upotrebu (CSIRT, regulatorna tijela)

2.9. Povezivanje sa modulom tretmana rizika

- Svaki procijenjeni rizik može biti proslijeđen modulu za tretman, gdje se definišu i implementiraju mjere za njegovo smanjenje.
- Sistem automatski prati efikasnost tretmana i prilagođava nivo rizika u skladu s primijenjenim mjerama.

3. Modul III „Upravljanje i tretman rizika”

Modul predstavlja ključni operativni segment softverskog sistema za sajber bezbjednost, koji omogućava univerzitetima u Crnoj Gori da definišu, implementiraju i nadgledaju odgovarajuće mjere zaštite u cilju ublažavanja ili uklanjanja identifikovanih i procijenjenih sajber rizika. Ovaj modul dolazi nakon faze identifikacije i procjene rizika i omogućava prelazak sa analize na konkretne akcije tretmana, osiguravajući da upravljanje sajber bezbjednošću ne ostane samo teorijsko, već dobije praktičnu i mjerljivu dimenziju.

Glavne funkcionalnosti modula:

3.1. Odabir strategije tretmana rizika

Softver pruža vodič za donošenje odluke o tretmanu, na osnovu unaprijed definisanih politika univerziteta i nivoa prihvatljivosti rizika.Za svaki identifikovani i procijenjeni rizik, korisnik bira jednu od četiri standardne strategije tretmana:

- *Izbjegavanje rizika* – ukidanje aktivnosti, sistema ili procesa koji nosi rizik.
- *Smanjenje rizika* – primjena tehničkih, organizacionih i/ili administrativnih mjera koje umanjuju vjerovatnoću i/ili uticaj rizika.

- *Transfer rizika* – prebacivanje odgovornosti na treću stranu (npr. kroz ugovore, osiguranje, outsourcing).
- *Prihvatanje rizika* – prihvatanje rezidualnog rizika bez dodatnih mjera, ako je u granicama tolerancije.

3.2. Definisanje plana tretmana rizika

Softver omogućava višestruke mjere po jednom riziku, uz hijerarhijsko grupisanje i praćenje njihovog efekta. Nakon izbora strategije, korisnik kreira plan tretmana**,** koji sadrži:

- Naziv i opis mjere/mjera koje će se primijeniti
- Tip mjere (tehnička, organizaciona, pravna, edukativna itd.)
- Ciljni rizik (nivo kojem se teži nakon tretmana)
- Odgovorno lice/jedinica za implementaciju
- Resurse potrebne za sprovođenje mjere (budžet, vrijeme, ljudi)
- Početak i kraj implementacije
- Indikatore uspješnosti (KPI-jevi)

3.3. Povezivanje sa kontrolnim mjerama

Modul omogućava izbor gotovih kontrola (šablona) ili unos novih, specifičnih za instituciju. Svaki plan tretmana povezuje se sa odgovarajućim kontrolama iz baze bezbjednosnih mjera, koje mogu uključivati:

- Ažuriranje softvera i zakrpe
- Jačanje autentifikacije (npr. MFA)
- Segmentaciju mreže
- Obuku zaposlenih i studenata
- Izradu i ažuriranje politika i procedura
- Uspostavljanje tehničkih servisa (npr. SIEM, DLP)

3.4. Praćenje implementacije mjera

Korisnici mogu unositi komentare, dokaze implementacije i dodatne napomene, što omogućava transparentnu i revizijsku dokumentaciju. Modul uključuje sistem upravljanja zadacima i rokovima, koji omogućava:

- Praćenje statusa svake mjere (planirano, u toku, završeno, odgođeno, neuspješno)
- Notifikacije i podsjetnike odgovornim osobama
- Pregled dinamike realizacije kroz Gantt grafikone ili vremenske linije
- Automatsku procjenu napretka u realizaciji plana tretmana

3.5. Re-evaluacija rizika nakon tretmana (Post-treatment risk review)

Modul koristi algoritme za automatsko ažuriranje rizika, uz uvid u pređašnje i sadašnje vrijednosti vjerovatnoće i uticaja. Po završetku mjera, sistem omogućava ponovnu procjenu rizika, u cilju:

- Provjere da li je ciljni nivo rizika postignut
- Evidentiranja ostvarenog efekta mjera

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
Gorica
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and
the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

- Odluke o daljim koracima (zatvaranje rizika, dodatne mjere, prihvatanje preostalog rizika)

3.6. Upravljanje prihvaćenim rizicima

Svi rizici se evidentiraju u posebnoj bazi „prihvaćenih rizika" uz vremensko ograničenje i periodični pregled. Za rizike koje je uprava odlučila da prihvati, modul omogućava:

- Dokumentovanje razloga prihvatanja (npr. nizak uticaj, trošak mjera previsok)
- Odobravanje od strane nadležnog tijela (npr. Savjet za sajber bezbjednost univerziteta)
- Praćenje promjena u kontekstu (ako se poveća prijetnja ili ranjivost, rizik se reaktivira)

3.7. Izvještaji i dashboard za upravljanje

Modul generiše niz automatskih izvještaja i vizualizacija, uključujući:

- Stanje sprovođenja plana tretmana po jedinici
- Ukupni broj aktivnih vs. tretiranih rizika
- Najčešće korišćene mjere i njihova uspješnost
- Rezidualni nivo rizika po kategorijama (tehnički, pravni, organizacioni)
- Dinamiku realizacije mjera (kasni, u roku, završeno)

Izvještaji se mogu koristiti za internu analizu, reviziju, i eksterno izveštavanje prema:

- Nacionalnom akademskom CSIRT-u
- Ministarstvu prosvjete, nauke i inovacija
- Regulatornim tijelima

3.8. Integracija sa drugim modulima i alatima

- Modul mora biti potpuno integrisan sa:
    - Modulom „Procjena i analiza rizika" (uzima ulazne podatke o rizicima)
    - Modulom za „Praćenje i izvještavanje" (vizualizuje napredak i ishode)

4. Modul IV „Praćenje i revizija"

Modul predstavlja završnu, ali kontinuiranu fazu u ciklusu upravljanja sajber bezbjednosnim rizicima, koja osigurava da su identifikovani, procijenjeni i tretirani rizici pravilno nadgledani kroz vrijeme, da se promjene u okruženju pravovremeno prepoznaju, i da se cjelokupan sistem bezbjednosti redovno evaluira i poboljšava. Za univerzitete u Crnoj Gori, ovaj modul ima poseban značaj jer omogućava transparentnost, odgovornost i stalno poboljšanje u upravljanju bezbjednosnim rizicima u obrazovnom, istraživačkom i administrativnom kontekstu.

Ključne funkcionalnosti modula:

4.1. Praćenje statusa rizika i mjera u realnom vremenu

- Modul omogućava dinamičko praćenje svih aktivnih, tretiranih i prihvaćenih rizika.

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
Gorica
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

- Prikazuje status svakog rizika:
  - *Aktivan – neadresiran*
  - *U tretmanu – mjere u toku*
  - *Zatvoren – rizik eliminisan*
  - *Prihvaćen – dokumentovana odluka*
- Takođe, prati status primijenjenih mjera zaštite i planova tretmana, sa informacijama o rokovima, odgovornim osobama i napretku.

Promjene se ažuriraju automatski u zavisnosti od:
- Unosa novih prijetnji ili ranjivosti
- Promjene tehničkih ili organizacionih kontrola
- Informacija dobijenih od Nacionalnog akademskog CSIRT-a

4.2. Automatsko generisanje obavještenja i podsjetnika

Ova funkcionalnost obezbjeđuje **proaktivno djelovanje**, a ne samo reaktivnu reakciju. Sistem generiše **notifikacije** i šalje e-mail podsjetnike u sljedećim slučajevima:
- Kada se približava rok za implementaciju mjere
- Kada rizik nije ažuriran određeni vremenski period
- Kada nova ranjivost utiče na već tretirani rizik
- Kada se detektuje neusaglašenost između procijenjenog rizika i stanja kontrola

4.3. Revizija i ponovno vrednovanje rizika

Modul omogućava periodičnu reviziju svakog rizika kroz unaprijed definisane cikluse (npr. svakih 6 ili 12 mjeseci), ili **ad-hoc reviziju** u slučaju:
- Izmjena u IT infrastrukturi ili procesima
- Implementacije novih kontrola
- Pojave nove prijetnje (npr. 0-day ranjivosti)
- Incidenta ili neuspjeha prethodnih mjera

Sistem automatski:
- Prikazuje prethodne i trenutne vrijednosti vjerovatnoće i uticaja
- Upoređuje rezidualne nivoe rizika tokom vremena
- Predlaže potrebu za ažuriranjem plana tretmana ili dodatne mjere

4.4. Upravljanje revizionim zapisima i istorijatom

Ova funkcionalnost je ključna za transparentnost, internu kontrolu i eksternu reviziju (npr. od strane regulatora ili nezavisnih auditora).
Svaka promjena unutar sistema (procjena, mjera, odluka, status) se evidentira kroz revizijski trag:
  - Ko je izvršio promjenu
  - Kada je promjena izvršena
  - Šta je promijenjeno (npr. povećana vjerovatnoća, dodata nova kontrola)
- Mogućnost filtriranja istorijata po:

- Riziku
- Organizacionoj jedinici
- Tipu intervencije (tretman, prihvatanje, izmjena kontrole)

4.5. Praćenje ključnih indikatora performansi (KPI)

- Modul uključuje dashboard sa indikatorima za ocjenu efikasnosti procesa upravljanja rizicima:
  - Procenat rizika koji su u roku tretirani
  - Broj prihvaćenih rizika u odnosu na ukupne
  - Broj mjera koje su uspješno sprovedene vs. zakasnjele
  - Prosječno vrijeme između detekcije i zatvaranja rizika
- Moguće je postaviti ciljne KPI vrijednosti i pratiti ostvarenje ciljeva bezbjednosti na nivou univerziteta ili pojedinačnih fakulteta.

4.6. Povezivanje sa incidentima i eksternim izvorima

- Modul omogućava povezivanje registrovanih rizika sa:
  - Sajber incidentima evidentiranim unutar univerziteta
  - Prijavama i preporukama CSIRT tima
  - Nacionalnim i međunarodnim bazama ranjivosti (npr. CVE, ENISA, NIST NVD)

4.7. Planiranje i izvođenje interne revizije sajber bezbjednosti

- Modul omogućava:
  - Planiranje revizija (na nivou univerziteta, fakulteta, sistema)
  - Izbor oblasti koje se provjeravaju (politike, procedure, implementacija mjera)
  - Unos revizorskih nalaza i preporuka
  - Praćenje realizacije preporuka kroz statusne liste
- Moguće je uključivanje eksternih revizora uz definisane korisničke pristupe i ograničenja.

4.8. Vizualizacija i izvještavanje

- Interaktivni dashboard-i i grafikoni prikazuju:
  - Trendove rizika kroz vrijeme
  - Nivoe rizika po jedinici, tipu prijetnje ili resursa
  - Revizorsku pokrivenost i uspješnost tretmana
- Mogućnost generisanja formalnih izvještaja za:
  - Internu bezbjednosnu komisiju
  - Rektorat i Senat
  - Ministarstvo, regulatorna tijela ili donatore

5. Modul V „Izvještavanje i transparentnost”

Modul predstavlja horizontalnu komponentu softverskog sistema za upravljanje sajber bezbjednosnim rizicima, koja omogućava univerzitetima u Crnoj Gori da kroz

pouzdane, strukturisane i prilagodljive izvještaje obezbijede vidljivost, odgovornost, informisanost i usaglašenost sa zakonodavstvom i standardima. Ovaj modul obezbjeđuje da svi procesi u vezi sa identifikacijom, procjenom, tretmanom i praćenjem rizika budu dokumentovani, dostupni i razumljivi različitim ciljnim grupama – od IT osoblja i uprava fakulteta, do CSIRT timova i regulatornih institucija.

Ključne funkcionalnosti modula:

5.1. Kreiranje automatskih izvještaja po modulima i temama

Modul omogućava generisanje izvještaja iz svih ostalih funkcionalnih modula, uključujući:

- *Izvještaj o identifikaciji rizika*
  - Lista svih identifikovanih prijetnji, ranjivosti i resursa
  - Veze između prijetnji i ranjivih sistema
- *Izvještaj o procjeni rizika*
  - Vjerovatnoća, uticaj, početni i rezidualni nivo rizika
  - Prioritizacija rizika po važnosti i organizacionoj jedinici
- *Izvještaj o tretmanu rizika*
  - Planirane i realizovane mjere
  - Statusi i odgovorna lica
- *Izvještaj o praćenju i reviziji*
  - Trenutni status rizika
  - Promjene u procjenama kroz vrijeme
  - Historija revizija i korektivnih aktivnosti

Svaki izvještaj može se generisati automatski, ručno ili zakazano (npr. mjesečno, kvartalno).

5.2. Interaktivni dashboard-i za menadžment i IT osoblje

Modul uključuje vizualne panele (dashboard-e) sa ključnim pokazateljima stanja sajber bezbjednosti na univerzitetu:

- Broj aktivnih vs. zatvorenih rizika
- Nivo rizika po fakultetima, IT sistemima i tipovima prijetnji
- Statusi implementacije mjera zaštite
- Trendovi kroz vrijeme (npr. broj rizika smanjen za 20% u odnosu na prethodni kvartal)
- „Top 10" rizika koji zahtijevaju hitnu pažnju

Dashboard-i su *interaktivni i prilagodljivi*, sa mogućnošću filtriranja po vremenskom okviru, jedinici, tipu resursa ili vrsti rizika.

5.3. Prilagođeni izvještaji za različite ciljne grupe

Modul omogućava generisanje izvještaja prilagođenih specifičnim korisnicima i njihovim potrebama:

- *Uprava univerziteta:* sažeti izvještaji sa ključnim pokazateljima i strateškim preporukama

- *IT sektor:* tehnički detaljni izvještaji o stanju infrastrukture, ranjivostima i neophodnim mjerama
- *Rektorski i dekanatski timovi:* pregled rizika i tretmana po organizacionim jedinicama
- *CSIRT timovi i eksterni partneri:* standardizovani izvještaji o bezbjednosnim incidentima i preduzetim akcijama
- *Regulatorna tijela i akreditacione komisije:* izvještaji usklađeni sa propisima (Zakon o informacionoj bezbjednosti, GDPR, NIST CSF)

Izvještaji se mogu izvoziti u više formata: PDF, Word, Excel, CSV

5.4. Usklađenost sa zakonodavstvom i standardima

Svi izvještaji koje generiše modul mogu biti oblikovani tako da budu usaglašeni sa regulatornim zahtjevima**:**

- Zakon o informacionoj bezbjednosti Crne Gore
- Zakon o zaštiti podataka o ličnosti (usaglašen sa GDPR)
- ISO/IEC 27001 i 27005
- NIST Cybersecurity Framework 2.0
- ENISA preporuke za obrazovni sektor

Ova funkcionalnost omogućava univerzitetima da dokumentuju svoju usklađenost sa relevantnim normama i budu spremni za inspekcije, akreditacije i međunarodne evaluacije.

5.5. Sistem kontrole pristupa izvještajima (Role-based Access)

- Pristup izvještajima je strogo kontrolisan kroz sistem uloga i dozvola:
  - Npr. IT administrator može vidjeti tehničke izvještaje za sve jedinice
  - Dekan može vidjeti samo izvještaje koji se odnose na njegov fakultet
  - Rektor i menadžment imaju uvid u konsolidovane izvještaje za cijeli univerzitet
- Obezbjeđena je zaštita osjetljivih podataka, posebno ako izvještaji sadrže informacije o ličnim podacima, istraživačkim resursima i tehničkim ranjivostima.

5.6. Praćenje transparentnosti i komunikacije

- Modul vodi evidenciju o tome:
  - Ko je kreirao, pregledao ili preuzeo izvještaj
  - Kojim institucijama je izvještaj proslijeđen (npr. Ministarstvo, CSIRT)
  - Da li su izvještaji upotrebljeni za donošenje odluka (uz napomene i zaključke)
- Ova evidencija omogućava izgradnju sistema odgovornosti i institucionalne kulture transparentnosti**.**

5.7. Integracija sa drugim modulima i vanjskim sistemima

- Automatsko povlačenje podataka iz modula:
  - Identifikacija rizika
  - Procjena i tretman
  - Praćenje i revizija
- Mogućnost integracije sa:

- Nacionalnim CSIRT-om
- Internim ERP sistemima univerziteta
- Sistemima za kvalitet i akreditaciju

6. Modul VI „Višenivovski pristup i decentralizovana upotreba"

Modul predstavlja ključnu funkcionalnost softverskog sistema za upravljanje sajber bezbjednosnim rizicima, posebno dizajniranu za kompleksnu organizacionu strukturu univerziteta u Crnoj Gori. Ovaj modul omogućava da se softver koristi istovremeno na više organizacionih nivoa – od centralnog IT sektora do pojedinačnih fakulteta, instituta, službi i organizacionih jedinica – uz kontrolisani pristup i jasno definisane odgovornosti. Takođe, omogućava upravljanje korisničkim pravima u skladu sa funkcionalnim ulogama korisnika, bez narušavanja bezbjednosti ili preklapanja ovlašćenja.

Ključne funkcionalnosti modula:

6.1. Višenivovska hijerarhija korisnika i organizacionih jedinica

Softver podržava kompleksnu strukturu univerziteta kroz hijerarhijski model koji uključuje:

- *Nivo univerziteta (centrala):* Rektorat, centralna IT i CSIRT služba, univerzitetski bezbjednosni timovi.
- *Nivo fakulteta i organizacionih jedinica:* Fakulteti, instituti, biblioteke, službe za informacione sisteme, laboratorije.
- *Nivo pojedinačnih sistema i servisa:* IT sistemi, aplikacije, mrežni čvorovi, platforme (npr. eLearning, SIS, IKT infrastruktura).

Svaka jedinica može raditi u okviru svoje instance sistema, a istovremeno biti integrisana u jedinstven univerzitetski okvir, čime se obezbjeđuje standardizovan pristup, ali decentralizovana primjena.

6.2. Uloge korisnika i granularna kontrola pristupa (Role-Based Access Control – RBAC)

Modul omogućava precizno definisanje korisničkih uloga i prava, na osnovu njihovih funkcija u instituciji:

- *Administrator sistema* – ima potpuni pristup svim podacima i konfiguracijama
- *Univerzitetski CSIRT tim* – pristup svim rizicima, incidentima i mjerama na nivou univerziteta
- *Fakultetski IT koordinator* – vidi i upravlja samo rizicima i mjerama svog fakulteta
- *Bezbjednosni službenik (ISO)* – nadgledanje kontrola, kreiranje izvještaja
- *Menadžeri i dekanati* – pristup agregiranim izvještajima i odlukama o tretmanu rizika
- *Korisnik/istraživač* – ograničeni uvid u procese koji se odnose na projekte ili sisteme kojima upravljaju

Moguće je dodati i prilagođene uloge, sa specifičnim pristupnim privilegijama na nivou funkcije, jedinice ili projekta.

6.3. Samostalni rad jedinica uz centralnu koordinaciju

Modul omogućava fakultetima i organizacionim jedinicama da samostalno:

- Identifikuju rizike i prijetnje
- Procjenjuju i tretiraju rizike
- Upravljaju lokalnim planovima mjera
- Generišu izvještaje relevantne za svoj nivo

Istovremeno, univerzitetski centar ima *centralizovani nadzor* nad:

- Stanjem svih rizika na nivou univerziteta
- Efikasnošću mjera po jedinicama
- Praćenjem dosljednosti primjene politike bezbjednosti

Ova kombinacija omogućava **lo**kalnu agilnost i centralnu odgovornost, što je ključno u složenim akademskim sistemima.

6.4. Delegiranje odgovornosti i tokovi odobravanja

Modul uključuje tokove odobravanja (approval workflows) koji podržavaju sljedeće scenarije:

- Fakultet definiše plan tretmana → prosljeđuje univerzitetskom CSIRT-u na potvrdu
- ISO unutar jedinice revidira identifikovani rizik → prosljeđuje rukovodstvu na odobrenje
- Dekanat može prihvatiti preostali rizik uz automatsku registraciju odluke

Ovi tokovi osiguravaju transparentnost, logičan slijed i odgovornost u donošenju bezbjednosnih odluka.

6.5. Prava pristupa po funkcionalnim modulima

Pristup se dodatno može ograničiti po tipu modula:

- Korisnik može imati pravo samo za „identifikaciju rizika“, ali ne i za „tretman“ ili „izvještavanje“
- Fakultetski timovi mogu vidjeti samo podatke koji se odnose na njihov organizacioni domen
- Revizori mogu imati samo „read-only“ pristup uz mogućnost komentarisanja

Ova fleksibilnost omogućava minimalni potrebni pristup u skladu sa načelima *Least Privilege Access* ***i*** *Need to Know*.

6.6. Zajednički i izolovani podaci

Modul podržava koncept:

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
Gorica
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

- *Zajedničkih podataka* – npr. baze prijetnji, tipova ranjivosti, predložene kontrole koje svi mogu koristiti
- *Izolovanih podataka* – podaci koji su dostupni samo unutar jedne organizacione jedinice (npr. informacije o specifičnoj ranjivosti laboratorijskog sistema)

Omogućena je i kontrolisana razmjena podataka između jedinica (npr. zajednički istraživački projekti na više fakulteta).

6.7. Zasebna i zajednička izvještavanja

- Svaka jedinica može:
  - Kreirati i čuvati vlastite izvještaje
  - Generisati izvještaje za interne potrebe ili eksternu akreditaciju
- Istovremeno, centralna instanca sistema omogućava:
  - Konsolidovane izvještaje za upravu univerziteta, CSIRT, ministarstvo
  - Poređenje učinka različitih jedinica (npr. procentualna pokrivenost planovima tretmana)

Time se obezbjeđuje horizontalna i vertikalna transparentnost.

7. Modul VII „Lokalizacija i usklađenost sa crnogorskim okvirom"

Ovaj modul obezbjeđuje da softverski sistem za procjenu, analizu i upravljanje sajber bezbjednosnim rizicima u potpunosti odgovara pravnom, institucionalnom, jezičkom i organizacionom kontekstu visokoškolskih ustanova u Crnoj Gori. Ovaj modul je ključan za prihvatanje i efikasno korišćenje softvera na nacionalnom nivou, jer omogućava da svi procesi, interfejsi, izvještaji, procedure i bezbjednosne politike budu u skladu sa važećim zakonima, strategijama, praksama i standardima u crnogorskom obrazovnom i informacionom prostoru.

Glavne funkcionalnosti modula:

7.1. Jezik sistema: crnogorski i engleski interfejs

- Kompletan korisnički interfejs (UI/UX), uključujući:
  - Meni opcije, forme, alatke
  - Poruke grešaka i potvrde
  - Objašnjenja, tutorijali, uputstva
- Dostupan je na:
  - *Crnogorskom jeziku* – za svakodnevnu upotrebu u akademskom okruženju
  - *Engleskom jeziku* – za potrebe međunarodnih partnerstava, revizora, EU projekata i akreditacionih tijela
- Modul omogućava prebacivanje jezika u realnom vremenu, bez potrebe za ponovnim pokretanjem sistema.

7.2. Terminološka prilagođenost crnogorskom obrazovnom i IT kontekstu

- Svi izrazi u softveru su prilagođeni:
  - Akademskoj terminologiji (npr. „fakultet", „studijski program", „istraživačka jedinica")
  - Tehničkoj i bezbjednosnoj terminologiji korišćenoj u nacionalnim dokumentima (npr. Strategija sajber bezbjednosti Crne Gore, zakon o IS)
- Ugrađeni su lokalni izrazi i fraze koji su razumljivi zaposlenima i menadžmentu univerziteta, kako bi se olakšalo korišćenje i smanjila jezička barijera.

7.3. Usklađenost sa crnogorskim zakonodavstvom i propisima

Softver je usklađen sa važećim i relevantnim zakonskim, regulatornim i strateškim dokumentima**,** uključujući:

- Zakon o informacionoj bezbjednosti Crne Gore
- Zakon o visokom obrazovanju
- Zakon o zaštiti podataka o ličnosti (usklađen sa GDPR)
- Zakon o elektronskoj upravi
- Strategija sajber bezbjednosti Crne Gore (2023–2027)
- Nacionalne politike digitalizacije, e-obrazovanja i bezbjednosti

Svaka funkcionalnost unutar softvera (npr. procjena rizika, evidencija incidenata, prava pristupa) implementirana je na način koji omogućava usklađenost sa zakonskim obavezama univerziteta.

7.4. Ugrađeni regulatorni i normativni šabloni

- Modul sadrži prilagođene šablone i obrasce za kreiranje dokumentacije u skladu sa crnogorskim standardima:
  - Politika informacione bezbjednosti
  - Planovi upravljanja rizicima
  - Evidencija o prihvaćenim rizicima
  - Obrasci za reviziju i izvještavanje
  - Incident report obrasci prema nacionalnom CSIRT-u

Svi obrasci su prilagođeni za štampu, potpis i digitalno arhiviranje, i mogu se eksportovati u PDF, Word i druge formate.

7.5. Integracija sa Nacionalnim akademskim CSIRT-om

- Sistem podržava razmjenu podataka i izvještaja sa:
  - Nacionalnim akademskim CSIRT-om
  - Ministarstvom prosvjete, nauke i inovacija
  - Relevantnim regulatornim tijelima
- Softver omogućava:

- Prijavu incidenata kroz standardizovane forme
- Prosljeđivanje izvještaja o rizicima i mjerama
- Komunikaciju o upozorenjima, preporukama i zahtjevima

Ova integracija omogućava univerzitetima da postanu aktivni dio nacionalnog sajber odbrambenog sistema.

7.6. Usklađenost sa crnogorskim akreditacionim zahtjevima

- Softver omogućava generisanje izvještaja i evidencija u formi potrebnoj za:
  - Nacionalnu akreditaciju studijskih programa
  - Institucionalnu akreditaciju i eksternu evaluaciju
  - Izvještavanje prema ENQA/EQAR okvirima
- Pruža podršku za dokazivanje:
  - Postojanja i primjene politika sajber bezbjednosti
  - Upravljanja rizicima u informacionim sistemima visokog obrazovanja
  - Integracije bezbjednosne kulture u nastavu, istraživanje i upravljanje

Ova funkcionalnost je od posebne važnosti za visokoškolske ustanove koje teže evropskoj i međunarodnoj prepoznatljivosti.

7.7. Usklađenost sa ISO i NIST standardima, lokalno prilagođena

- Iako koristi međunarodne norme (ISO 27001/27005, NIST CSF 2.0), softver ih interpretira u kontekstu crnogorskog sistema kroz:
  - Lokalno primjenjive kontrole i procedure
  - Prilagođene matrice vjerovatnoće i uticaja
  - Lokalizovane politike upravljanja rizicima
- Time se omogućava kombinacija globalnih standarda i lokalne primjene.

8. Modul VIII „Integracija sa nacionalnim akademskim CSIRT-om”

Ovaj modul predstavlja ključnu komponentu softverskog sistema za upravljanje sajber bezbjednosnim rizicima na univerzitetima u Crnoj Gori, omogućavajući direktnu, sigurnu i efikasnu komunikaciju i koordinaciju između univerzitetskih IT i bezbjednosnih timova i Nacionalnog akademskog CSIRT-a (Computer Security Incident Response Team). Ova integracija je od izuzetne važnosti za pravovremeno otkrivanje, prijavu i reagovanje na sajber prijetnje i incidente, kao i za kontinuiranu razmjenu informacija o bezbjednosnim rizicima i preporukama na nacionalnom nivou.

Ključne funkcionalnosti modula:

8. 1. Automatizovana prijava bezbjednosnih incidenata

- Omogućava univerzitetskim CSIRT ili IT timovima da direktno prijave incidente Nacionalnom akademskom CSIRT-u putem integrisanih elektronskih obrazaca unutar softvera.
- Podržava različite tipove incidenata (malver, DDoS napadi, phishing, kompromitacija naloga, neautorizovani pristup, itd.).
- Podaci o incidentu uključuju detalje o vremenu, tipu, pogođenim sistemima, mjestima otkrivanja i poduzetim prvim koracima.

Sistem osigurava da su podaci sigurno i šifrovano preneseni prema Nacionalnom CSIRT-u, u skladu sa sigurnosnim standardima.

8.2. Primanje i sinhronizacija upozorenja i preporuka (Alerts & Advisories)

- Softver prima i automatski sinhronizuje sigurnosna upozorenja, obavještenja o ranjivostima i preporuke Nacionalnog akademskog CSIRT-a**.**
- Upozorenja se prikazuju korisnicima sistema u realnom vremenu kroz posebne notifikacije ili unutar dashboard-a.
- Preporuke za mjere i kontrole mogu se direktno povezati sa aktivnim rizicima i planovima tretmana na univerzitetu.

8.3. Dvosmjerna komunikacija i saradnja

- Omogućava direktnu razmjenu poruka i dokumenata između univerzitetskih timova i Nacionalnog akademskog CSIRT-a.
- Podržava slanje zahtjeva za pomoć, dodatne informacije ili koordinaciju akcija tokom upravljanja incidentima.
- Omogućava Nacionalnom CSIRT-u da šalje povratne informacije, sugestije i hitne obavijesti korisnicima sistema.

Ova funkcionalnost jača brzu koordinaciju i zajednički odgovor na prijetnje.

8.4. Automatizovana razmjena podataka o rizicima i kontrolama

- Softver šalje Nacionalnom akademskom CSIRT-u ažurirane informacije o identifikovanim rizicima, trenutnom stanju tretmana i efektima primijenjenih mjera**.**
- Omogućava Nacionalnom CSIRT-u da koristi ove podatke za analizu ukupnog nivoa bezbjednosti u akademskom sektoru i planiranje nacionalnih akcija.

8.5. Integracija sa Nacionalnom bazom ranjivosti i prijetnji

- Modul omogućava pristup i automatsku sinhronizaciju sa centralizovanim nacionalnim bazama ranjivosti, prijetnji i incidenata koje održava Nacionalni akademski CSIRT.
- Podaci se koriste za pravovremenu identifikaciju novih prijetnji koje mogu uticati na univerzitete.
- Omogućava automatsku procjenu uticaja novih ranjivosti na univerzitetske sisteme i servise.

8.6. Standardizovani formati za razmjenu informacija

- Koristi se interoperabilni format za razmjenu bezbjednosnih informacija, kao što su:
  - STIX (Structured Threat Information eXpression)
  - TAXII (Trusted Automated eXchange of Indicator Information)
  - CVE (Common Vulnerabilities and Exposures)
- Time je obezbijeđena kompatibilnost sa drugim nacionalnim i međunarodnim CSIRT timovima i sigurnosnim platformama.

8.7. Sigurnosne politike i kontrole pristupa

- Pristup modulima integracije je ograničen samo na ovlašćene korisnike sa posebnim privilegijama.
- Svi podaci koji se razmjenjuju su zaštićeni enkripcijom i praćeni revizijskim zapisima.
- Implementirane su kontrole za sprječavanje curenja osjetljivih podataka i neautorizovanog pristupa.

8.8. Evidencija i izvještavanje o komunikaciji sa CSIRT-om

- Modul vodi detaljnu evidenciju o svim aktivnostima koje uključuju razmjenu informacija sa Nacionalnim akademskim CSIRT-om:
  - Kada je incident prijavljen
  - Ko je i kada izvršio prijavu
  - Primljene povratne informacije i preporuke
- Generišu se izvještaji o saradnji sa CSIRT-om za potrebe unutrašnje kontrole i eksternih revizija.

Opšti zahtjevi

1. Upravljanje korisničkim identitetima

Korisničke identitete i naloge treba objediniti sa postojećim bazama (npr. LDAP katalozima) korisnika, identiteta i naloga. Odluka o rješenjima koja će se primjeniti zavisi od situacije na terenu i tehničkih mogućnosti univerziteta.

2. Aplikativne uloge

Aplikativne uloge (role) za pristup aplikaciji treba prilagoditi vrstama korisnika sistema i akcijama u sistemu na koje oni tipično imaju pravo. Funkcionalnosti treba realizovati tako da se jednostavno mogu pridružiti prethodno definisanim rolama za pristup.

3. Obim i automatizacija obrade podataka

Softver treba da omogući:

- Rad u bilo kom trenutku, aktivnost 24 časa dnevno, 7 dana u nedelji;
- Rad do 150 istovremenih korisnika po univerzitetu;
- Automatsko generisanje i štampanje svih potrebnih dokumenata na zahtjev korisnika.
- Pretragu, filtriranje i izvoz odabranih podataka u Excel, CSV ili PDF format;

4. Bezbjednosni zahtjevi

Neophodno je da svi podaci budu locirani na serveru sa adekvatnom zaštitom od neovlašćenog pristupa.

- Komunikacija putem sigurnih protokola (HTTPS, TLS 1.2+).
- Enkripcija podataka u tranzitu i mirovanju (AES-256).
- Dvofaktorska autentifikacija (MFA) za privilegovane korisnike.
- Redovan backup i disaster recovery plan.
- Detekcija neautorizovanog pristupa i neobičnog ponašanja.

5. Tehničke specifikacije

Tehničke karakteristike softverskog rešenja:

Stavka	**Zahtjev**
Tehnologija	Web-based
Baza podataka	PostgreSQL ili MySQL, MS SQL
Podržani browseri	Chrome, Firefox, Edge (najnovije verzije)
Deployment	On-premise ili u edukativnom cloudu (preference naručioca)
Lokalizacija	Podrška za crnogorski i engleski jezik
Skalabilnost	Modularna arhitektura, podrška za više univerziteta ili jedinica
Pristup mobilnim uređajima	Responsivni dizajn, mobile-friendly interfejs

Softver mora imati opciju za:

- Automatska obavještenja (e-mail, SMS)
- Trening modul za edukaciju korisnika
- API pristup za eksternu integraciju
- AI podršku za preporuke kontrola (poželjno, ali ne obavezno)

6. Dokumentacija i podrška

- Dokumentacija podrazumijeva cjelokupan izvorni kod aplikativnog, kao i propratne dokumente koji sadrže tehničke detalje implementacije rješenja, što uključuje sljedeće elemente: arhitektura sistema, komponente i njihove odgovornosti, tokovi podataka, spoljni interfejs sistema i formati podataka/lista za uvoz ili izvoz. Pruženi podaci treba da budu dovoljni za operativnu administraciju i održavanje sistema.
- Softver mora biti isporučen sa:
  - Korisničkim uputstvom (na crnogorskom i engleskom jeziku)
  - Administratorskim priručnikom
  - Tehničkom dokumentacijom API-ja
- Usluga inicijalne obuke korisnika i administratora
- Garancija i tehnička podrška 24 mjeseca tj. do kraja CSupMNE projekta

7. Instalacija

Instalacija rješenja podrazumijeva instalaciju i konfiguraciju rešenja na odabranoj lokaciji unutar Crne Gore. Po uspješno sprovedenoj instalaciji, konfigurisanju i obuci administratora sistema, sistem se pušta u rad.

8.Održavanje

- Garancija i tehnička podrška 24 mjeseca tj. do kraja CSupMNE projekta
- Korekcija uočenih nedostataka u funkcionalnostima koje su realizovane tokom realizacije rešenja, pruženo održavanje uključuje i unos inicijalnih podataka sa univerziteta, kao i ostalih relevantnih institucija na nacionalnom nivou, prilagođavanje rješenja eventualnim izmjenama u softverskim komponentama koje rješenje koristi.
- Izmjene koje su posljedica naknadnih promjena u poslovnom procesu ili imaju za cilj da zadovolje dodatne i naknadne zahtjeve fakulteta ili korisnika se mogu ugovoriti, s time da su te modifikacije i proširenja njihovo održavanje nezavisni od ovdje opisanog održavanja.

Opis Tehničkih zahtjeva korisnika za
Izradu softvera za Podršku u radu Nacionalnog akademskog CSIRT-a
za potrebe realizacije Erasmus + projekta
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
„Straightening Up Cybersecuirty Posture of Montenegrin Higheer Education System“

Uvodne napomene

Softver za podršku radu Nacionalnog akademskog CSIRT-a Crne Gore (Computer Security Incident Response Team) predstavlja digitalno rješenje razvijeno s ciljem da omogući efikasno, strukturirano i koordinisano upravljanje sajber bezbjednosnim incidentima u visokoškolskom sektoru**.** Ovaj softver omogućava Nacionalnom akademskom CSIRT-u da obavlja svoju ključnu ulogu u zaštiti univerzitetskih informacionih sistema kroz centralizovano prikupljanje, analizu, razmjenu i odgovor na bezbjednosne incidente i prijetnje, u tesnoj saradnji sa univerzitetima, istraživačkim centrima i drugim akterima akademskog okruženja.

Kao alat usklađen sa najboljim međunarodnim praksama (CERT/CSIRT standardima), nacionalnim zakonodavstvom i strategijama sajber bezbjednosti, softver omogućava CSIRT timu da:

- Upravljanje događajima i incidentima (Event & Incident Management).
- Upravljanje ranjivostima.
- Situacionu svest i razmenu informacija.
- Obuku, treninge i transfer znanja

Softver je u **potpunosti** lokalizovan za crnogorski kontekst, sa višejezičnim interfejsom (crnogorski i engleski), integracijom sa univerzitetskim sistemima, kao i podrškom za nacionalne propise i tehničke standarde. Kroz modularan dizajn, sistem omogućava skalabilnost, interoperabilnost i jednostavno upravljanje svim fazama odgovora na incidente, čime značajno doprinosi jačanju sajber otpornosti akademskog sektora Crne Gore**.**

Glavni elementi softvera za Podršku u radu Nacionalnog akademskog CSIRT-a

Softver za podršku radu Crnogorskog Nacionalnog akademskog CSIRT-a sastoji se od više međusobno povezanih modula koji omogućavaju obavljanje svih ključnih funkcija jednog CSIRT tima u sektoru visokog obrazovanja – od prijema prijava i upravljanja

incidentima, preko analize prijetnji i ranjivosti, do komunikacije, izvještavanja, koordinacije i dokumentovanja procesa.

Softver za podršku radu Crnogorskog Nacionalnog akademskog CSIRT-a (NA-CSIRT) sastoji se iz sledećih ključnih modula:

- **Modul I: Informacioni bezbjednosni događaji (Information Security Event Management)**. Ovaj modul predstavlja osnovu za rano otkrivanje potencijalnih incidenata kroz analizu podataka prikupljenih kontinuiranim nadzorom informacionih sistema. Glavni cilj je omogućiti CSIRT timu i organizaciji da pravovremeno identifikuju anomalije i potencijalne prijetnje, smanjujući rizik od ozbiljnijih incidenata. Modul obuhvata ključni servis i funkciju: Prihvatanje događaja za analizu sa kvalifikacijom događaja radi razlikovanja stvarnih incidenata od lažnih alarma.
- **Modul II: Upravljanje incidentima (Information Security Incident Management)**. Cilj ovog modula je da obezbedi efikasnu obradu, analizu i koordinaciju u slučaju sigurnosnih incidenata, omogućavajući organizacijama da brzo reaguju i minimiziraju posledice. Servisi uključuju prijem i potvrdu prijava incidenata, triage i inicijalnu obradu prijava kako bi se identifikovali prioriteti, i analizu incidenata koja obuhvata kategorizaciju, prioritetizaciju, prikupljanje dokaza i korelaciju incidenata. Funkcije podrške za mitigaciju i oporavka omogućavaju planiranje odgovora, ad-hoc mere kao i podrška za povraćaj sistema i podataka. Osnovna funkcija Modula je koordinacija i komunikacija, uključujući interne i eksterne kanale (TLP), generisanje notifikacija i izveštaja, medijsku komunikaciju, kao i podršku kriznom menadžmentu kroz distribuciju statusa i strateških odluka. Softverski zahtevi uključuje modul za lifecycle incidenata, portal za prijave incidenata i automatizovana izvještavanja koja omogućavaju brzo donošenje odluka i transparentnost procesa.
- **Modul III: Upravljanje ranjivostima (Vulnerability Management)**. Ovaj modul je fokusiran na prihvatanje prijava za isporuku servisa analize i odgovor na ranjivosti u informacionim sistemima, čime se smanjuje površina za potencijalne napade. Servis uključuje koordinaciju sa vendorima i partnerima**,** kao i objavljivanje i distribuciju saveta **z**a ranjivosti (vulnerability disclosure) kako bi se zajednica obavestila o prijetnjama i preporučenim merama. Odgovor na ranjivosti uključuje korišćenje skenera, remedijaciju i patch management, čime se efikasno zatvaraju sigurnosni propusti.
- **Modul IV: Situaciona svest (Situational Awareness)**. Cilj ovog modula je proaktivno razumevanje pretnji i pružanje informacija akademskoj zajednici i korisnicima sistema kako bi se povećala spremnost i smanjio rizik od incidenata. Servisi obuhvataju prikupljanje podataka kroz policy mapping, asset mapping i integraciju sa threat intelligence feedovima, analizu i sintezu podataka radi identifikacije trendova incidenata i pružanja podrške u odlučivanju, kao i komunikaciju kroz izveštaje, preporuke i razmenu informacija sa ključnim akterima.
- **Modul V: Transfer znanja (Knowledge Transfer)**. Ovaj modul ima za cilj edukaciju, podizanje svesti i jačanje kapaciteta korisnika i članova organizacije. Servisi

uključuju podizanje svesti kroz kampanje, newsletter-e i izveštaje o pretnjama, obuku i edukaciju kroz kurseve, e-learning platforme i mentoring programe, kao i savjetodavne usluge vezane za upravljanje rizicima i podršku u kreiranju politika. Softverski zahtevi uključuju e-learning modul, repozitorijum znanja i alat za generisanje izveštaja, čime se omogućava kontinuirana edukacija, povećava otpornost organizacije i jačaju veštine u upravljanju incidentima.

Detaljni prikaz modula

1. Modul I – Upravljanje događajima informacione bezbednosti

Upravljanje događajima informacione bezbednosti (Information Security Event Management – ISEM) ima za cilj prihvatanje za analizu događaja prikupljenih iz različitih izvora podataka. U većim organizacijama, funkcije ovog modula se često dodeljuju Centru za operativnu bezbednost (SOC), koji može obavljati i prvostepeno ili drugostepeno upravljanje incidentima, uključujući iniciranje mera za ublažavanje rizika ili prilagođavanje bezbednosnih kontrola.

Interfejs između SOC-a i dodeljenog CSIRT-a je od ključnog značaja, jer sve usluge upravljanja incidentima zavise od kvalifikovanih i tačnih podataka o bezbednosnim događajima.

U okviru modula I izdvaja se jedna glavna usluga: Prihvatanje događaja za analizu

1.1. Prihvatanje događaja za analizu

Svrha: Servis analize događaja obuhvata trižiranje i kvalifikaciju detektovanih potencijalnih incidenata kako bi se omogućila pravovremena eskalacija u servis upravljanja incidentima ili označavanje kao lažnih alarma.
Opis: Tok potencijalnih incidenata se trižira, a svaki incident se kvalifikuje kao stvarni incident (true positive) ili lažni alarm (false positive) koristeći manuelnu i/ili automatizovanu analizu. Prioritet se daje kritičnijim incidentima kako bi se omogućila pravovremena reakcija. Struktuirana kvalifikacija omogućava kontinuirano unapređenje detekcionih slučajeva, izvora podataka i procesa.
Ishod: Kvalifikovani i korelisani incidenti informacione bezbednosti dostupni su za dalju obradu u okviru servisa upravljanja incidentima, dok se lažni pozitivni rezultati koriste za unapređenje procesa detekcije i analize.

Funkcije servisa:

1. *Prihvatanje i Kvalifikacija* – trižiranje i kategorizacija potencijalnih incidenata, određivanje prioriteta i procena rizika. Automatizacija omogućava efikasno obogaćivanje kontekstom, identifikaciju ponavljajućih slučajeva i unapređenje procesa detekcije.

Ishod: Kvalifikovani potencijalni incidenti informacione bezbednosti spremni su za rukovanje u okviru servisa upravljanja incidentima, omogućavajući pravovremenu reakciju i unapređenje bezbednosnih procesa.

2. Modul II – Upravljanje incidentima informacione bezbednosti

Upravljanje incidentima informacione bezbednosti (Information Security Incident Management – ISIM) ima za cilj efikasnu obradu, analizu i koordinaciju u slučaju incidenata, čime se minimizuju posledice po organizaciju i njene korisnike. Modul II predstavlja centralni servis CSIRT-a ili SOC-a u kojem se svi prijavljeni incidenti analiziraju, kategorizuju, tretiraju i dokumentuju u skladu sa definisanim procedurama i standardima.

2.1 – Prijem i inicijalna obrada incidenata

- *Svrha:* Omogućava pravovremeno prijemanje i inicijalnu obradu incidenata informacione bezbednosti, osiguravajući da svaki incident bude pravilno registrovan i prosleđen odgovarajućem timu.
- *Opis:* Prijem i potvrda prijave obuhvataju evidentiranje incidenta, identifikaciju izvora i tipa incidenta, inicijalnu analizu i određivanje prioriteta (triage). Cilj je da incident bude pravilno klasifikovan i pripremljen za dalje analize.
- *Ishod:* Incident je registrovan i prosleđen odgovarajućem timu za dalju obradu.

Funkcije servisa:

1. *Prijem i potvrda prijave* – evidentiranje incidenata iz različitih izvora, po prijavi korisnika.
2. *Triage i inicijalna obrada* – određivanje prioriteta, identifikacija kritičnih incidenata i prosleđivanje na odgovarajuće resurse.

2.2 – Analiza incidenata

- *Svrha:* Omogućava analizu prijavljenih incidenata kako bi se identifikovali uzroci, procenio rizik i planirale odgovarajuće reakcije.
- *Opis:* Analiza obuhvata kategorizaciju, prikupljanje dokaza, korelaciju sa drugim incidentima i identifikaciju root cause. Cilj je precizno razumevanje incidenta kako bi se obezbedila pravovremena i adekvatna reakcija.
- *Ishod:* Incident je detaljno analiziran i pripremljen za forenzičku obradu ili implementaciju mera mitigacije.

Funkcije servisa:

1. *Kategorizacija i prioritetizacija* – određivanje tipa i kritičnosti incidenta.
2. *Prikupljanje informacija* – formiranje repozitorijuma dokaza (logs, capture files, network traces).
3. *Root cause analiza i korelacija* – identifikacija uzroka incidenta i povezivanje sa sličnim incidentima ili prethodnim događajima.

European Commission Erasmus+ Project:
ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027 / 101179688
Gorica
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made
| **PROJECT COORDINATOR:** University of Donja
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

2.3 – Mitigacija i oporavak

Svrha: Omogućava implementaciju mera za smanjenje uticaja incidenata i povratak sistema u normalno stanje.
Opis: Uključuje izradu plana odgovora, ad-hoc mere, izolaciju kompromitovanih sistema i povraćaj podataka i funkcionalnosti.
Ishod: Incident je neutralisan, a sistemi i podaci vraćeni u sigurno i funkcionalno stanje.
Funkcije servisa:

1. *Plan odgovora* – definisanje standardnih i prilagođenih koraka za reakciju na incident.
2. *Ad-hoc mere i izolacija* – trenutne intervencije radi sprečavanja širenja incidenata.
3. *Povraćaj sistema i podataka* – obnavljanje kompromitovanih resursa i osiguranje kontinuiteta poslovanja.

2.4 – Koordinacija i komunikacija

Svrha: Omogućava efikasnu internu i eksternu koordinaciju tokom incidenta, uključujući izveštavanje i komunikaciju sa ključnim zainteresovanim stranama.
Opis: Servis obuhvata komunikaciju putem sigurnih kanala (TLP), notifikacije, izveštaje i medijsku komunikaciju kada je relevantno.
Ishod: Osigurana je pravovremena informisanost i koordinacija svih relevantnih strana, čime se povećava efikasnost odgovora.
Funkcije servisa:

1. *Interna i eksterna komunikacija* – koordinacija između CSIRT tima, korisnika i eksternih partnera.
2. *Notifikacije i izvještaji* – formalno dokumentovanje i prosleđivanje informacija.
3. *Medijska komunikacija* – upravljanje informacijama prema javnosti i medijima u slučaju većih incidenata.

2.5 – Podrška kriznom menadžmentu

Svrha: Podrška u strateškom donošenju odluka tokom incidenta i kriznih situacija.
Opis: Obuhvata distribuciju statusa i izveštaja menadžmentu i podršku u komunikaciji strateških odluka.
Ishod: Krizni menadžment ima ažurne i precizne informacije za donošenje odluka, čime se minimizira poslovni rizik i potencijalna šteta.

3. Modul III – Upravljanje ranjivostima

Upravljanje ranjivostima (Vulnerability Management) ima za cilj prijem zahtjeva za identifikaciju, analizu i pravovremeno reagovanje na ranjivosti u informacionim sistemima i infrastrukturnim komponentama. Modul III omogućava CSIRT-u i organizaciji da proaktivno smanji rizik od napada i kompromitacije, koordinisanjem aktivnosti otkrivanja, prijema, analize i remedijacije ranjivosti.

3.1. Prijem zahtjeva za otkrivanje ranjivosti

Svrha: Prijem zahtjeva za realizaciju identifikovanje ranjivosti u softveru, mrežama i sistemima kako bi se smanjila mogućnost iskorišćavanja od strane napadača.
Opis: Prijem zahtjeva kako bi se koordinisale različite metode, uključujući automatizovane skenere, fuzzing, istraživanja i OSINT izvore, radi detekcije potencijalnih slabosti.
Ishod: Identifikovane su ranjivosti koje zahtevaju dalju analizu ili hitnu remedijaciju.
Funkcije servisa:

1. *Prijem zahtjeva za otkrivanje ranjivosti* – za redovno i ciljno otkrivanje ranjivosti na svim kritičnim resursima.
2. *Analiza i prioritetizacija* –procena uticaja i vejrovatnoće iskorišćavanja ranjivosti

3.2. Prijem i analiza izveštaja o ranjivostima

Svrha: Upravljanje spoljašnjim i internim prijavama ranjivosti, uključujući koordinaciju sa vendorima i partnerima.
Opis: Uključuje verifikaciju, kategorizaciju i root cause analizu prijavljenih ranjivosti, te pripremu preporuka za mitigaciju.
Ishod: Ranjivosti su validirane i pripremljene za remedijaciju, dok je informacija o njima adekvatno distribuirana odgovarajućim akterima.
Funkcije servisa:

1. *Prijem izveštaja o ranjivostima* – konsolidacija prijava iz različitih izvora.
2. *Validacija i kategorizacija* – potvrda postojanja ranjivosti i određivanje njenog značaja.
3. *Koordinacija sa vendorima i partnerima* – osiguranje komunikacije o pravovremenm ispravkama i distribuciji zakrpa.

3.3. Odgovor i remedijacija

Svrha: Isporuka preporuka za tehničke i proceduralne mjere radi smanjenja rizika od eksploatacije identifikovanih ranjivosti.
Opis: Uključuje preporuke za patch management, konfiguracione izmene i preporuke za sigurnosne kontrole.
Ishod: Ranjivosti su sanirane ili kontrolisane, čime se povećava ukupna bezbednost organizacije.
Funkcije servisa:

1. *Isporuka preporuka ua Patch management, Remedijaciju,* – preporuke za implementaciju zakrpa i ažuriranja softverskih komponenti primjena drugih tehničkih mera ili promena konfiguracije za smanjenje rizika.

4. Modul IV – Situaciona svest

Situaciona svest (Situational Awareness) predstavlja proaktivno praćenje, analizu i informisanje akademske zajednice ili organizacije o trenutnim i potencijalnim pretnjama. Modul IV omogućava donošenje pravovremenih i informisanih odluka baziranih na relevantnim podacima o incidentima i trendovima.

4.1. Prikupljanje podataka

Svrha: Obezbeđuje kontinuirani protok relevantnih informacija o prijetnjama, resursima i rizicima.
Opis: Podaci se prikupljaju iz izvora kao što su politike, asset mapping, threat intelligence feedovi i drugi relevantni sistemi.
Ishod: Organizacija ima sveobuhvatnu bazu podataka koja omogućava pravovremeno reagovanje na pretnje.
Funkcije servisa:

1. *Prikupljanje podataka iz internih i eksternih izvora* – mapiranje resursa i politika, praćenje feedova.
2. *Upravljanje threat intel podacima* – filtriranje, normalizacija i kategorizacija informacija.

4.2. Analiza i sinteza

Svrha: Omogućava identifikaciju trendova, projekcija i donošenje odluka na osnovu podataka.
Opis: Obuhvata analitičke metode i sintezu informacija radi kreiranja trendova, scenarija i preporuka za bezbednosne odluke.
Ishod: Pripremljeni su izveštaji i analitički materijali koji podržavaju upravljanje rizikom i planiranje bezbednosnih aktivnosti.
Funkcije servisa:

1. *Projekcije i trendovi incidenata* – identifikacija obrazaca i potencijalnih budućih incidenata.
2. *Decision support* – priprema podataka i preporuka za menadžment i korisnike.

4.3. Komunikacija

Svrha: Distribucija i razmena informacija u cilju podizanja svesti i pripreme zajednice na pretnje.
Opis: Uključuje izradu izveštaja, preporuka i deljenje informacija sa relevantnim akterima unutar i izvan organizacije.
Ishod: Akademska zajednica ili organizacija dobija pravovremene i relevantne informacije o bezbednosnim rizicima.
Funkcije servisa:

1. *Izrada izveštaja i preporuka* – priprema profesionalnih dokumenata i materijala.

| **PROJECT COORDINATOR:** University of Donja Gorica
| Donja Gorica, 81 000 Podgorica, Montenegro
| http://www.udg.edu.me / | udg@udg.edu.me
| Tel:+382(0)20 410 777 | Fax:+382(0)20 410 766

2. *Razmena informacija i koordinacija* – omogućava bolje razumevanje pretnji i unapređuje saradnju među zainteresovanim stranama.

5. Modul V – Transfer znanja

Modul V – Transfer znanja (Knowledge Transfer) ima za cilj podizanje svesti, edukaciju i obuku korisnika, kao i prenos iskustava i najboljih praksi u oblasti informaciono-bezbednosnih incidenata i upravljanja rizicima. Kroz ovaj modul CSIRT omogućava da organizacija i njeni članovi bolje razumeju pretnje, uče kako da ih prepoznaju, spreče ili ublaže i kako da adekvatno reaguju u slučaju incidenta.

5.1. Podizanje svesti

Svrha: Povećanje sveukupnog nivoa bezbednosti kroz kontinuiranu edukaciju i informisanje korisnika o aktuelnim pretnjama i najboljim bezbednosnim praksama.
Opis: Servis obuhvata kampanje, newsletter-e, izveštaje i druge forme komunikacije koje podižu svest o bezbednosnim rizicima i merama zaštite. Fokus je na pružanju praktičnih uputstava za prepoznavanje i reagovanje na incidente.
Ishod: Korisnici i zaposleni bolje razumeju bezbednosne rizike i postupke za njihovo ublažavanje, što smanjuje verovatnoću uspešnih napada i incidenata.
Funkcije servisa:

1. *Istraživanje i analiza informacija* – prikupljanje relevantnih podataka o pretnjama i trendovima.
2. *Izrada materijala za podizanje svesti* – kreiranje prezentacija, infografika, video materijala i izveštaja.
3. *Distribucija i komunikacija* – deljenje materijala kroz interne kanale, web portale, društvene mreže ili kampanje.

5.2. Obuka i edukacija

Svrha: Osposobljavanje članova organizacije i CSIRT-a za prepoznavanje, prevenciju i reagovanje na bezbednosne incidente.
Opis: Programi obuke mogu uključivati kurseve, e-learning, radionice, mentoring i simulacije. Obuka je prilagođena različitim nivoima korisnika, od tehničkog osoblja do menadžmenta, kako bi svi relevantni akteri razvili potrebna znanja, veštine i sposobnosti (KSAs).
Ishod: Korisnici i zaposleni stiču praktične i teorijske veštine potrebne za identifikaciju i reagovanje na incidente, kao i za primenu sigurnosnih politika i procedura.
Funkcije servisa:

1. *Prikupljanje zahteva za znanje, veštine i sposobnosti (KSAs)* – identifikacija potreba i kompetencija korisnika.
2. *Razvoj edukativnih i obučnih materijala* – kreiranje sadržaja kao što su prezentacije, vodiči, simulacije i online kursevi.

3. *Dostava sadržaja* – organizovanje kurseva, radionica, e-learning sesija, hands-on laboratorija i CTF (capture the flag) takmičenja.
4. *Mentoring* – omogućavanje učenja kroz formalne i neformalne mentorske programe.
5. *Profesionalni razvoj CSIRT osoblja* – kontinuirano usavršavanje i praćenje novih trendova i tehnologija u oblasti bezbednosti.

5.3. Savetodavne usluge

Svrha: Podrška organizaciji u oblasti upravljanja rizicima, politike i procedura, kao i tehničkih pitanja vezanih za informacionu bezbednost.
Opis: CSIRT pruža savetodavne usluge kako bi se poboljšale interne politike, implementacija standarda i strategija zaštite, uključujući podršku u incident managementu i poslovnoj kontinuitetu.
Ishod: Organizacija je sposobna da donosi informisane odluke o bezbednosti, implementira najbolje prakse i adekvatno reaguje na pretnje.
Funkcije servisa:

1. *Podrška u upravljanju rizicima* – identifikacija pretnji i predlaganje mera kontrole.
2. *Podrška za kontinuitet poslovanja i oporavak od katastrofa* – razvoj i implementacija planova.
3. *Savetodavna podrška za politike* – kreiranje, institucionalizacija i implementacija bezbednosnih politika.
4. *Tehnička podrška i preporuke* – saveti za alate, infrastrukturu i bezbednosne procedure.

Opšti zahtjevi

1. Upravljanje korisničkim identitetima

Korisničke identitete i naloge treba objediniti sa postojećim bazama (npr. LDAP katalozima) korisnika, identiteta i naloga. Odluka o rješenjima koja će se primjeniti zavisi od situacije na terenu i tehničkih mogućnosti univerziteta.

2. Aplikativne uloge

Aplikativne uloge (role) za pristup aplikaciji treba prilagoditi vrstama korisnika sistema i akcijama u sistemu na koje oni tipično imaju pravo. Funkcionalnosti treba realizovati tako da se jednostavno mogu pridružiti prethodno definisanim rolama za pristup.

3. Obim i automatizacija obrade podataka

Softver treba da omogući:

- Rad u bilo kom trenutku, aktivnost 24 časa dnevno, 7 dana u nedelji;
- Rad do 150 istovremenih korisnika po univerzitetu;
- Automatsko generisanje i štampanje svih potrebnih dokumenata na zahtjev korisnika.
- Pretragu, filtriranje i izvoz odabranih podataka u Excel, CSV ili PDF format;

4. Bezbjednosni zahtjevi

Neophodno je da svi podaci budu locirani na serveru sa adekvatnom zaštitom od neovlašćenog pristupa.

- Komunikacija putem sigurnih protokola (HTTPS, TLS 1.2+).
- Enkripcija podataka u tranzitu i mirovanju (AES-256).
- Dvofaktorska autentifikacija (MFA) za privilegovane korisnike.
- Redovan backup i disaster recovery plan.
- Detekcija neautorizovanog pristupa i neobičnog ponašanja.

5. Tehničke specifikacije

Tehničke karakteristike softverskog rešenja:

Stavka	**Zahtjev**
Tehnologija	Web-based
Baza podataka	PostgreSQL ili MySQL, MS SQL
Podržani browseri	Chrome, Firefox, Edge (najnovije verzije)
Deployment	On-premise ili u edukativnom cloudu (preference naručioca)
Lokalizacija	Podrška za crnogorski i engleski jezik
Skalabilnost	Modularna arhitektura, podrška za više univerziteta ili jedinica
Pristup mobilnim uređajima	Responsivni dizajn, mobile-friendly interfejs

Softver mora imati opciju za:

- Automatska obavještenja (e-mail, SMS)
- Trening modul za edukaciju korisnika
- API pristup za eksternu integraciju
- AI podršku za preporuke kontrola (poželjno, ali ne obavezno)

6. Dokumentacija i podrška

- Dokumentacija podrazumijeva cjelokupan izvorni kod aplikativnog, kao i propratne dokumente koji sadrže tehničke detalje implementacije rješenja, što uključuje sljedeće elemente: arhitektura sistema, komponente i njihove odgovornosti, tokovi podataka, spoljni interfejs sistema i formati podataka/lista za uvoz ili izvoz. Pruženi podaci treba da budu dovoljni za operativnu administraciju i održavanje sistema.
- Softver mora biti isporučen sa:
  - Korisničkim uputstvom (na crnogorskom i engleskom jeziku)
  - Administratorskim priručnikom
  - Tehničkom dokumentacijom API-ja
- Usluga inicijalne obuke korisnika i administratora
- Garancija i tehnička podrška 24 mjeseca tj. do kraja CSupMNE projekta

7. Instalacija

Instalacija rješenja podrazumijeva instalaciju i konfiguraciju rešenja na odabranoj lokaciji unutar Crne Gore. Po uspješno sprovedenoj instalaciji, konfigurisanju i obuci administratora sistema, sistem se pušta u rad.

8.Održavanje

- Garancija i tehnička podrška 24 mjeseca tj. do kraja CSupMNE projekta
- Korekcija uočenih nedostataka u funkcionalnostima koje su realizovane tokom realizacije rešenja, pruženo održavanje uključuje i unos inicijalnih podataka sa univerziteta, kao i ostalih relevantnih institucija na nacionalnom nivou, prilagođavanje rješenja eventualnim izmjenama u softverskim komponentama koje rješenje koristi.
- Izmjene koje su posljedica naknadnih promjena u poslovnom procesu ili imaju za cilj da zadovolje dodatne i naknadne zahtjeve fakulteta ili korisnika se mogu ugovoriti, s time da su te modifikacije i proširenja njihovo održavanje nezavisni od ovdje opisanog održavanja.