VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

VLOGA VARNOSTNO-OPERATIVNIH CENTROV PRI ODKRIVANJU, PREPREČEVANJU IN ANALIZI KIBERNETSKIH DOGODKOV V SLOVENSKEM IN EVROPSKEM PROSTORU

Kandidat: Matic Šebjan Ogrizek

Vrsta študija: študent izrednega študija

Študijski program: Računalništvo

Mentor predavatelj: dr. Simon Žnidar, univ. dipl. inž. el.

Mentor v podjetju: Marko Zavadlav, univ. dipl. inž. rač. in inf.

Lektorica: Anja Ivančič, dipl. slov. in germ.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Matic Šebjan Ogrizek sem avtor diplomskega dela z naslovom Vloga varnostno-operativnih centrov pri odkrivanju, preprečevanju in analizi kibernetskih dogodkov v slovenskem in evropskem prostoru, ki sem ga napisal pod mentorstvom Simona Žnidarja. S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot mojih lastnih – kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Ljubljana, september 2025 Podpis študenta:

ZAHVALA

Zahvaljujem se svoji partnerki Simoni za pomoč, podporo in navdih pri pisanju diplomske naloge. Iskrena hvala mentorju, dr. Simonu Žnidarju, za vso pomoč, usmeritve in dragocene povratne informacije pri nastajanju dela. Posebno se zahvaljujem mentorju v podjetju, Marku Zavadlavu, za pomoč pri pripravi gradiva, temeljit pregled diplomske naloge in stalno podporo. Zahvaljujem se tudi vodji VOC, Petru Hutniskemu, za pregled strukture VOC in za uvajanje na delovno mesto varnostnega analitika.

POVZETEK

Diplomsko delo obravnava vlogo varnostno-operativnih centrov (VOC) pri odkrivanju, preprečevanju in analizi kibernetskih dogodkov v slovenskem in širšem evropskem prostoru. Izhodišče predstavlja vprašanje, katere organizacijske, procesne in tehnične značilnosti ločijo zrel VOC od reaktivno organiziranega varnostnega nadzora ter kako te razlike vplivajo na odpornost organizacij. Uporabljena metodologija združuje pregled standardov in smernic, primerjalno analizo evropskih praks ter sintezo spoznanj v vzorčni delovni protokol VOC.

Rezultati kažejo, da je tipična struktura VOC sestavljena iz ravni od 1 do 3 in vodje VOC. Prva raven skrbi za neprekinjen nadzor, triažo in validacijo dogodkov, druga raven vodi poglobljene tehnične preiskave ter usklajuje z nosilci infrastrukture, tretja raven izvaja lov na grožnje, digitalno forenziko in razvoj detekcij, vodja VOC pa upravlja prioritetizacijo, kadrovske zmogljivosti in komunikacijo. V primerjavi z najzrelejšimi evropskimi okolji slovenske organizacije najpogosteje zaostajajo v kadrovski širini, stopnji specializacije, uvedbi orkestracije in avtomatizacije, neprekinjeni pokritosti ter doslednem merjenju uspešnosti. Kljub temu je opazen jasen trend standardizacije, profesionalizacije in približevanja najboljšim praksam. Učinkovit odziv v realnem času zahteva kakovostno vidljivost procesov (telemetrija SIEM/XDR/EDR/UEBA, dnevniški zapisi, CTI), vnaprej definirane postopke z jasnimi vlogami in pogoji eskalacije, orkestracijo rutinskih korakov ter redno učenje na podlagi incidentov (*lessons learned*). NIS 2 in nacionalne politike VOC postavljajo v vlogo operativnega nosilca skladnosti z zahtevami po pravočasnem poročanju, obvladovanju tveganj in neprekinjenem delovanju. Posebej pomembni so upravljanje tveganj dobaviteljev ter vnaprej dogovorjena izmenjava informacij in sodelovanje z nacionalnimi institucijami, kot je CSIRT.

Praktični prispevek dela je vzorčni delovni protokol VOC, ki standardizira organizacijo izmen, operativne postopke, komunikacijske poti, vodenje evidenc in povezavo s standardi ter regulativo. Omejitve izhajajo iz zaupnosti internih podatkov in heterogenosti okolij; nadaljnje raziskave naj kvantificirajo učinke avtomatizacije in primerjajo modele delovanja (*in-house*, MSSP/MDR, hibrid).

Ključne besede: *varnostno-operativni center, VOC, kibernetska varnost, NIS 2, SIEM, SOAR*

ABSTRACT

The Role of Security Operations Centers (SOCs) in Detecting, Preventing, and Analyzing Cyber Incidents in the Slovenian and European Context

This thesis examines the role of Security Operations Centers (SOC) in detecting, preventing, and analyzing cyber incidents in Slovenia and Europe. It asks which organizational, process, and technical characteristics distinguish a mature SOC from a reactive security monitoring function, and how these differences affect organizational resilience. The methodology combines a review of relevant standards and guidelines, a comparative analysis of European practices, and the synthesis of findings into a model SOC operating protocol.

Findings indicate that a typical SOC structure is organized around Levels 1–3 and an SOC manager: Level 1 provides 24/7 monitoring, triage, and event validation; Level 2 conducts in-depth technical investigations and coordinates with infrastructure owners; Level 3 performs threat hunting, digital forensics, and detection engineering; the manager oversees prioritization, workforce capacity, metrics, and communication. Compared with the most mature European environments, Slovenian organizations most commonly lag in staffing depth, specialization, orchestration and automation, round-the-clock coverage, and consistent performance measurement. Nonetheless, there is a clear trend toward standardization, professionalization, and alignment with best practices. Effective real-time response requires high-quality visibility (telemetry from SIEM/XDR/EDR/UEBA, log data, and cyber threat intelligence), predefined procedures with clear roles and escalation criteria, orchestration of routine steps, and systematic post-incident learning. At the regulatory level, the NIS 2 Directive and national implementations position the SOC as an operational pillar of compliance, including timely reporting, risk management, and continuity obligations. Supplier-risk management and pre-agreed information sharing with national CSIRTs are especially important.

The practical contribution of the thesis is a model SOC operating protocol that standardizes shift organization, operational procedures, communication paths, record-keeping, and linkage to standards and regulation. Limitations arise from the confidentiality of internal SOC data and the heterogeneity of environments; future research should quantify automation impacts and compare operating models (in-house, MSSP/MDR, hybrid).

Keywords: *Security Operations Center (SOC), cybersecurity, NIS 2, SIEM, SOAR, incident response*

KAZALO VSEBINE

Uporabljene kratice

- VOC: varnostno-operativni center
- SOC (Security Operations Center): varnostno-operativni center
- SIEM (Security Information and Event Management): upravljanje varnostnih informacij in dogodkov
- SOAR (Security Orchestration, Automation and Response): orkestracija, avtomatizacija in odziv na varnostne dogodke
- NIS 2 (Directive on measures for a high common level of cybersecurity): direktiva NIS 2 o ukrepih za visoko skupno raven kibernetske varnosti
- ZInfV-1: Zakon o informacijski varnosti
- CSIRT (Computer Security Incident Response Team): ekipa za odziv na varnostne incidente
- CERT (Computer Emergency Response Team): ekipa za odziv v računalniških izrednih dogodkih
- ENISA (European Union Agency for Cybersecurity): Agencija EU za kibernetsko varnost
- CTI (Cyber Threat Intelligence): obveščevalni podatki o kibernetskih grožnjah
- EDR (Endpoint Detection and Response): odkrivanje in odziv na končnih točkah
- XDR (Extended Detection and Response): razširjeno odkrivanje in odziv
- UEBA (User and Entity Behavior Analytics): analitika vedenja uporabnikov in entitet
- IDS (Intrusion Detection System): sistem za odkrivanje vdorov
- IPS (Intrusion Prevention System): sistem za preprečevanje vdorov
- NDR (Network Detection and Response): omrežno odkrivanje in odziv
- IR (Incident Response): odziv na incidente
- DFIR (Digital Forensics and Incident Response): digitalna forenzika in odziv na incidente
- IOC (Indicator of Compromise): indikator kompromitacije
- MTTD (Mean Time To Detect): povprečni čas do zaznave

- MTTR (Mean Time To Respond/Recover): povprečni čas do odziva/okrevanja
- SOP (Standard Operating Procedure): standardni operativni postopek
- Playbook (Incident Response Playbook): operativni priročnik/izvedbeni načrt za incident
- KPI (Key Performance Indicator): ključni kazalnik uspešnosti
- KRI (Key Risk Indicator): ključni kazalnik tveganja
- SLA (Service Level Agreement): sporazum o ravni storitve
- MSSP (Managed Security Service Provider): upravljani ponudnik varnostnih storitev
- MDR (Managed Detection and Response): upravljano odkrivanje in odziv
- ISMS (Information Security Management System): sistem upravljanja informacijske varnosti
- ISO/IEC 27001 (Information Security Management Systems – Requirements): mednarodni standard za sisteme upravljanja informacijske varnosti
- GDPR (General Data Protection Regulation): Splošna uredba o varstvu podatkov
- TLP (Traffic Light Protocol): protokol semafor
- STIX (Structured Threat Information Expression): strukturiran zapis za izmenjavo podatkov o grožnjah
- TAXII (Trusted Automated Exchange of Intelligence Information): zaupanja vreden avtomatiziran prenos podatkov o grožnjah
- IAM (Identity and Access Management): upravljanje identitet in dostopov
- PAM (Privileged Access Management): upravljanje privilegiranih dostopov
- RBAC (Role-Based Access Control): nadzor dostopa na podlagi vlog
- MFA (Multi-Factor Authentication): večfaktorska avtentikacija
- VPN (Virtual Private Network): navidezno zasebno omrežje
- DLP (Data Loss Prevention): preprečevanje izgube podatkov
- CVE (Common Vulnerabilities and Exposures): seznam znanih ranljivosti in izpostavljenosti

- CWE (Common Weakness Enumeration): katalog pogostih šibkosti
- NVD (National Vulnerability Database): nacionalna baza ranljivosti (ZDA)
- BCP (Business Continuity Plan): načrt neprekinjenega poslovanja
- DORA (Digital Operational Resilience ACT): Uredba o digitalni operativni odpornosti za finančni sektor
- IKT: informacijsko-komunikacijska tehnologija
- ZInfV-1: Zakon o informacijski varnosti
- ZVOP: Zakon o varstvu osebnih podatkov

1 UVOD

Vloga varnostno-operativnih centrov v sodobni digitalni družbi postaja vse pomembnejša, saj se organizacije na vseh ravneh soočajo z naraščajočim številom kibernetskih groženj. Kibernetski napadi niso več omejeni zgolj na posamezne hekerske skupine, temveč vključujejo tudi organizirane kriminalne združbe in državne akterje, kar povečuje njihovo resnost in posledice.

1.1 Opis področja in opredelitev problema

V sodobnem digitalnem okolju so organizacije vse bolj izpostavljene različnim oblikam kibernetskih groženj, ki lahko ogrozijo poslovanje, zaupnost, celovitost in razpoložljivost podatkov ter varnost kritične infrastrukture. Varnostno-operativni centri (angl. Security Operations Centers – SOC), v slovenskem prostoru poznani tudi kot VOC, predstavljajo ključno točko za zaznavanje in odzivanje na kibernetske dogodke ter za njihovo preprečevanje. Njihova naloga ni zgolj tehnične narave, temveč vključuje tudi strateško upravljanje tveganj, usklajevanje z zakonodajo ter sodelovanje z nacionalnimi in mednarodnimi varnostnimi organi.

Kljub vse večji uporabi avtomatizacije in naprednih orodij ostaja vloga človeškega faktorja ključna pri analizi kompleksnih incidentov in sprejemanju odločitev. Slovenija si prizadeva slediti evropskim trendom, vendar se v praksi VOC med seboj močno razlikujejo po zrelosti, strukturi, uporabljenih tehnologijah in načinu delovanja.

1.2 Namen, cilji in osnovne trditve

Namen naloge je raziskati vlogo varnostno-operativnih centrov pri odkrivanju, preprečevanju in analizi kibernetskih dogodkov v slovenskem in širšem evropskem prostoru. Poseben poudarek bo na strukturi VOC, pomembnosti človeškega faktorja, učinkovitosti odziva, usklajenosti z direktivo NIS 2 in sodelovanju z zunanjimi deležniki.

Cilji naloge so:

- predstaviti strukturo dela analitikov na VOC po različnih ravneh (nivoji 1, 2, 3 in vodje);
- opredeliti pomen človeškega faktorja v okolju, kjer se uporablja avtomatizacija;
- analizirati uporabo ključnih varnostnih orodij in učinkovitost odziva na incidente;
- ovrednotiti zrelost slovenskih VOC v primerjavi z evropskimi praksami;

– preučiti usklajenost z direktivo NIS 2 in upravljanje tveganj glede tretjih strani;
– raziskati sodelovanje z nacionalnimi in evropskimi varnostnimi organi;
– oblikovati pogled na razvoj VOC v prihodnosti.

Hipoteze, ki ji bom skozi potek diplomskega dela zavrgel ali potrdil:

– H1: Vsi delovni protokoli v VOC niso dovolj jasno dokumentirani.
– H2: Standardizirani protokoli dela so ključni za učinkovito delovanje VOC v kriznih situacijah.
– H3: Ustrezno dokumentirani protokoli zmanjšujejo odvisnost od posameznih izkušenih zaposlenih.
– H4 (dodatna hipoteza): BTEC 2025 »Kibernetska varnost«: Uvajanje novih zaposlenih v VOC je hitrejše in učinkovitejše, če organizacija uporablja dokumentiran protokol dela in s tem skrbi za kibernetsko higieno.

Raziskovalna vprašanja, ki jih bom ovrednotil:

1. Kakšna je zrelost VOC v Sloveniji v primerjavi z razvitejšimi evropskimi državami?
2. Kako pomembna je prisotnost človeškega faktorja v okoljih VOC kljub avtomatizaciji?
3. Kako VOC zagotavljajo odziv na incidente v realnem času in kakšna je njihova učinkovitost?
4. Kako pomembna je vloga sistemov za odkrivanje, preprečevanje in analizo kibernetskih dogodkov pri vsakodnevnem delu analitika na VOC?
5. V kolikšni meri se slovenske in evropske organizacije prilagajajo zahtevam direktive NIS 2, ki ureja področje kibernetske varnosti?
6. Kako organizacije v Sloveniji upravljajo tveganja glede tretjih strani (dobaviteljskih verig) znotraj operacij VOC?
7. Kakšno vlogo ima sodelovanje VOC z nacionalnimi in evropskimi varnostnimi organi?
8. Kako se bo po pričakovanjih razvijala vloga VOC v naslednjih letih v Sloveniji in Evropi?
9. Kakšno vlogo ima delovni protokol pri zagotavljanju učinkovitega delovanja varnostno-operativnega centra pri zaznavanju, obvladovanju in preprečevanju kibernetskih incidentov?

10. Kako lahko strukturiran delovni protokol prispeva k izboljšanju sodelovanja med različnimi deležniki znotraj VOC in z zunanjimi partnerji?
11. Kaj pomeni fleksibilnost za uspešnost izvajanja storitev VOC? (Placeholder1)

1.3 Predpostavke in omejitve

V nalogi se predpostavlja, da intervjuvani strokovnjaki in dostopna literatura predstavljajo reprezentativen vpogled v delovanje VOC v Sloveniji in Evropi. Omejitev predstavlja dostopnost podrobnejših informacij o notranjih postopkih VOC zaradi zaupnosti podatkov. Poleg tega so lahko razlike med državami pogojene s pravnim okvirom, razpoložljivimi sredstvi in stopnjo digitalizacije.

1.4 Uporabljene raziskovalne metode

Naloga temelji na kombinaciji kvalitativnih in kvantitativnih metod. Uporabljeni bodo:

– analiza strokovne literature in zakonodajnih dokumentov (npr. direktiva NIS 2, ZInfV),
– primerjalna analiza izbranih VOC v Sloveniji in Evropi,
– intervjuja s strokovnjakoma v VOC,
– analiza sekundarnih podatkov (študija primerov, poročila agencij, varnostne analize ...).

2 STRUKTURA IN DELOVANJE VARNOSTNO-OPERATIVNIH CENTROV (VOC)

V današnjem svetu se organizacije soočajo z vse bolj sofisticiranimi in vse pogostejšimi kibernetskimi grožnjami, ki lahko povzročijo resne posledice za poslovanje in varnost podatkov. Varnostno-operativni centri (VOC) igrajo ključno vlogo pri zaščiti informacijskih sistemov ter hitrem in učinkovitem odzivanju na kibernetske incidente. Zaradi naraščajoče kompleksnosti grožnje je nujno, da organizacije vzpostavijo jasno strukturiran in učinkovit VOC, ki omogoča sistematično spremljanje, analizo in odzivanje na varnostne dogodke. Razumevanje organizacijske strukture VOC je pomembno za zagotavljanje optimalne delitve nalog in učinkovite koordinacije med posameznimi nivoji analitikov. Določitev jasnih vlog in odgovornosti omogoča učinkovito delovanje centra ter povečuje zmožnost zaznavanja in reševanja incidentov v realnem času. Prav tako je pomembno razumeti razlike v strukturi VOC med Slovenijo in drugimi evropskimi državami, saj primerjava razkriva področja, kjer se slovenske prakse lahko izboljšajo. To poglavje zato nudi podrobno opredelitev koncepta VOC, opisuje organizacijsko strukturo teh centrov ter primerja različne pristope k njihovi organiziranosti v Sloveniji in Evropi. Nadalje se osredotoča na specifične naloge in odgovornosti posameznih ravni analitikov, kar omogoča jasen pregled delovnih procesov znotraj VOC.

2.1 Opredelitev koncepta VOC

Varnostno-operativni centri (VOC), v angleškem jeziku poimenovani *Security Operations Centers (SOC)*, predstavljajo ključno točko za obravnavo kibernetskih groženj v organizaciji. Osnovni namen VOC so centralizirano spremljanje, odkrivanje, analiza in odzivanje na kibernetske incidente, s čimer se zagotavlja visoka raven informacijske varnosti. VOC se osredotoča na zaščito ključnih informacijskih virov, preprečevanje incidentov in čim hitrejše reševanje problemov v realnem času (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

2.2 Struktura in organizacija VOC

VOC so običajno organizirani po hierarhičnih nivojih, imenovanih tudi *tier*s, izmed katerih ima vsak specifične naloge, pristojnosti in stopnje zahtevnosti.

- *Tier 1 (nivo 1) – začetni nivo analize (Alert Monitoring and Triage)*: na nivoju 1 analitiki opravljajo osnovno spremljanje varnostnih opozoril, ki jih generirajo različni varnostni sistemi, kot je Security Information and Event Managment (SIEM). Njihove naloge so hitro vrednotenje opozoril, začetna klasifikacija groženj in eskalacija primerov na višji nivo analize, če to situacija zahteva. Njihovo delo je zelo rutinsko, strukturirano in temelji na vnaprej definiranih postopkih (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).
- *Tier 2 (nivo 2) – poglobljena analiza in odzivanje (Incident Analysis and Response)*: na nivoju 2 analitiki obravnavajo primere, ki so eskalirali s prvega nivoja. Naloge nivoja 2 vključujejo bolj poglobljeno tehnično analizo, identifikacijo izvora in obsega incidentov ter koordinacijo odziva. Prav tako skrbijo za dokumentiranje incidentov in tesno sodelujejo z IT-ekipami za odpravljanje posledic napadov. Njihovo delo zahteva bolj specializirano znanje ter uporabo naprednih analitičnih orodij in postopkov (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).
- *Tier 3 (nivo 3) – napredna tehnična podpora in specializirana analiza (Advanced Technical Support)*: analitiki na tem nivoju predstavljajo najvišji nivo tehničnega znanja v VOC. Ukvarjajo se z najkompleksnejšimi grožnjami, izvajajo poglobljene forenzične analize in povratni inženiring zlonamerne kode. Prav tako opravljajo proaktivno iskanje groženj (*Threat Hunting*), kjer iščejo indikatorje kompromitacije, ki jih osnovni sistemi za odkrivanje groženj ne zaznajo (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).
- *Nivo managerja (SOC Manager)*: managerji v VOC so odgovorni za upravljanje celotnega delovanja VOC. Skrbijo za koordinacijo med posameznimi nivoji, zagotavljajo vire za nemoteno delovanje, oblikujejo strategije, načrtujejo odziv na večje incidente in vzdržujejo odnose z zunanjimi partnerji, vključno z regulativnimi organi in drugimi organizacijami za kibernetsko varnost (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

2.3 Primerjava tipičnih struktur VOC v Sloveniji in Evropi

V Sloveniji so VOC pogosto manjši, z omejenim številom analitikov, kar vpliva na organizacijo dela. Slovenski VOC imajo običajno poenostavljeno hierarhično strukturo, kjer pogosto prihaja do združevanja vlog, zlasti med nivojema 1 in 2. V Evropi, zlasti v razvitih državah, so VOC

večji in bolj specializirani. Posamezni nivoji so jasno opredeljeni, kar omogoča večjo učinkovitost in globino analize. Evropski centri pogosto vlagajo tudi v napredne tehnologije in avtomatizacijo, ki omogočajo večjo odzivnost in natančnejšo analizo kibernetskih dogodkov (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

2.4 Specifika nalog in odgovornosti posameznih ravni analitikov

Učinkovitost delovanja varnostno-operativnega centra je veliki meri odvisna od jasne delitve nalog in odgovornosti med posameznimi ravnmi analitikov. Vsak nivo, od nivoja 1 do vodstva, ima svojo vlogo znotraj odzivnega mehanizma, ki deluje v realnem času in v zahtevnem okolju stalne pripravljenosti. Spodaj so predstavljene podrobnejše naloge po posameznih stopnjah hierarhije VOC.

Specifika nalog nivoja 1:

- Spremljanje varnostnih anomalij v realnem času. Analitiki na nivoju 1 neprestano nadzorujejo dogodke, ki jih generirajo varnostni sistemi, in iščejo morebitna odstopanja od običajnega vedenja sistemov.
- Osnovno vrednotenje in razvrščanje opozoril. Vsako opozorilo je analizirano glede na resnost, verjetnost ogroženosti in morebitne vplive ter nato razvrščeno po prioriteti.
- Eskalacija incidentov na višji nivo analize. Ko analitiki zaznajo sumljiv dogodek, ki presega njihovo raven obravnave, incident s pripadajočo dokumentacijo in komentarji predajo analitikom na nivoju 2.
- Redno vzdrževanje dokumentacije incidentov. Vodijo ažurno evidenco vseh dogodkov, opozoril in svojih postopkov odziva, kar je ključno za kasnejšo analizo in revizijo (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

Specifika nalog nivoja 2:

- Izvedba podrobne tehnične analize incidentov. Vključuje preiskavo izvora napada, obsega okužbe in prizadetih sistemov na podlagi dnevnikov in analitičnih orodij.
- Koordinacija odziva s sistemskimi in varnostnimi ekipami. Skupaj z drugimi IT-strokovnjaki izvajajo tehnične ukrepe, kot so izolacija sistemov, spremembe požarnih zidov in deaktivacija računov.

- Podpora pri odpravljanju posledic kibernetskih napadov. Pomagajo pri vzpostavitvi normalnega stanja, testiranju obnovljenih sistemov in izvajanju popravkov.
- Aktivno sodelovanje v procesu izboljšanja varnostnih politik in pristopov. Prispevajo k izboljšavam notranjih protokolov na osnovi pridobljenih izkušenj iz analiziranih incidentov (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

Specifika nalog nivoja 3:

- Napredna forenzična analiza in analiza zlonamerne programske opreme. Uporabljajo specializirana orodja za analizo binarnih kod, sistemskih sprememb in omrežnih tokov.
- Izvajanje naprednih tehnik groženj (angl. *Threat Hunting*). Aktivno iščejo neodkrite grožnje, ki bi se lahko skrivale v sistemih, in identificirajo nove vzorce napadov.
- Razvoj in implementacija novih metod in orodij za izboljšanje varnosti. Oblikujejo lastne skripte in avtomatizacije za optimizacijo odkrivanja groženj in poročanja.
- Svetovanje vodstvu glede strateških varnostnih ukrepov. Na podlagi analiz in trendov predlagajo strateške usmeritve in investicije v varnostno infrastrukturo (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

Specifika nalog nivoja managerja:

- Upravljanje operativnih in strateških aktivnosti VOC. Koordinirajo celotno delovanje centra, določajo prioritete in nadzorujejo izvajanje nalog.
- Zagotavljanje virov in opreme za učinkovito delovanje centra. Skrbijo za ustrezno kadrovsko strukturo, orodja in financiranje centrov.
- Komunikacija z zunanjimi deležniki in regulatornimi organi. Predstavljajo organizacijo v dialogu z državnimi institucijami, partnerji in industrijskimi združenji.
- Nadzor izvajanja politike skladnosti in vodenje tveganj. Redno izvajajo presoje, spremljajo skladnost z zakonodajo, kot je direktiva NIS 2, in nadzorujejo tveganja, povezana z informacijsko varnostjo (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

Poleg osnovnega razumevanja nalog je pomembno poznati tudi kompetence in orodja, ki jih analitiki na različnih ravneh uporabljajo. Na primer, analitiki nivoja 1 potrebujejo osnovno znanje o omrežnih protokolih, logičnem razmišljanju in orodjih za nadzor, kot je Qradar ali Splunk. Nivo 2 zahteva napredno razumevanje operacijskih sistemov, skript v Pythonu in PowerShellu ter poznavanje orodij za analizo, kot sta VirusTotal in SOCRadar. Analitiki na nivoju 3 pogosto posedujejo certifikate, kot so OSCP, GREM ali GIAC, in uporabljajo forenzična orodja, kot so OSForenzik, Velociraptro ali Nessus. Managerji pa morajo poleg vodstvenih sposobnosti razumeti standarde, kot so ISO 27001, NIST in direktiva NIS 2, ter imeti sposobnost vodenja krizne komunikacije in priprave strateških poročil za nadzorne odbore (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

3 PRAVNI IN STRATEŠKI OKVIR VOC V SLOVENIJI IN EVROPI

Zaradi naraščajočega števila in resnosti kibernetskih incidentov so države Evropske unije sprejele številne zakonodajne in strateške ukrepe, katerih cilj je povečati skupno odpornost na kibernetske grožnje. Varnostno-operativni centri (VOC) imajo ključno vlogo pri izvajanju teh ukrepov, saj so odgovorni za zaznavanje, preprečevanje, obravnavo in poročanje o kibernetskih incidentih. Pravni in strateški okvir v Sloveniji in Evropi določa obveznosti, standarde in smernice, ki jih morajo VOC upoštevati, da bi delovali skladno z zakonodajo in zagotavljali visoko stopnjo zaščite informacijskih sistemov.

V zadnjih letih so se na evropski ravni oblikovali različni mehanizmi za okrepitev kibernetske varnosti, pri čemer direktiva NIS 2 predstavlja osrednji steber novega regulatornega okolja. Njene naloge so uskladiti in okrepiti zmogljivosti držav članic na področju kibernetske zaščite, spodbuditi izmenjavo informacij med javnimi in zasebnimi subjekti ter zagotoviti hitro odzivanje na incidente. VOC morajo v tem okviru prevzeti osrednjo vlogo pri operativnem izvajanju ukrepov in pri oblikovanju organizacijskih struktur, ki so odporne na sodobne grožnje.

3.1 Pregled relevantnih pravnih regulatornih okvirjev

Eden najpomembnejših pravnih instrumentov na področju kibernetske varnosti je direktiva (EU) 2022/2555 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, bolj znana kot direktiva NIS 2 (EU, 2022). Gre za prenovljeno in bistveno okrepljeno različico direktive NIS iz leta 2016, ki uvaja številne nove obveznosti in mehanizme nadzora. Direktiva predpisuje oblikovanje nacionalnih strategij, vzpostavitev pristojnih nacionalnih organov, izboljšanje usposobljenosti centrov CSIRT ter jasno opredeljuje obveznosti poročanja in obvladovanja tveganj za ključne subjekte, kamor sodijo tudi VOC (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

VOC morajo po tej direktivi zagotavljati:

- redno ocenjevanje in upravljanje kibernetskih tveganj,
- izvajanje tehničnih in organizacijskih varnostnih ukrepov (npr. segmentacija omrežij, varnostne kopije, dostop na osnovi najmanjših privilegijev),

- poročanje o varnostnih incidentih najkasneje v 24 urah od njihove zaznave,
- sodelovanje z nadzornimi organi in izmenjavo informacij v realnem času.

V Sloveniji je implementacija direktive NIS 2 potekala prek Zakona o informacijski varnosti (ZInfV-1), ki je bil sprejeta leta 2025. Ta zakon določa tudi pooblastila Urada Vlade RS za informacijsko varnost kot osrednjega regulativnega telesa, odgovornega za izvajanje nadzora nad zavezanci in za koordinacijo nacionalnih aktivnosti na področju informacijske varnosti (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

3.2 Praksa skladnosti z direktivo NIS 2 v Sloveniji in Evropi

Skladnost z direktivo NIS 2 v praksi zahteva celostni pristop, ki vključuje pravno, tehnično in organizacijsko uskladitev vseh zavezancev. V Sloveniji so se večja podjetja in kritična infrastruktura (telekomunikacije, energetika, bančništvo) že prilagodili novim zahtevam, medtem ko so mala in srednja podjetja ter številni javni zavodi šele na začetku poti. Kljub temu se krepi sodelovanje z nacionalnim odzivnim centrom SI-CERT, ki nudi tehnično podporo in sodeluje pri usposabljanju kadra (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

V naprednejših evropskih državah, kot so Nizozemska, Nemčija, Finska in Estonija, je skladnost z direktivo že zelo visoka. Ti sistemi vključujejo digitalno identiteto za vse uporabnike, centralizirane nadzorne sisteme in avtomatizirano poročanje incidentov v realnem času. Nadzorni organi v teh državah izvajajo redne presoje, simulacije napadov (*red team/blue team*) in izdajajo kazni ob nespoštovanju zakonodaje. Poleg tega obstaja trend k večji interoperabilnosti nacionalnih sistemov znotraj EU, kar omogoča boljše upravljanje groženj in koordinacijo odzivov (ENISA, 2024).

Primer dobre prakse predstavlja francoski sistem ANSSI, ki poleg regulatorne vloge izvaja tudi tehnično podporo za podjetje, organizira nacionalne vaje in razvija odprtokodne rešitve za zaznavanje groženj. Podoben sistem obstaja tudi v Nemčiji (BSI), ki ima pod svoje okrilje vključene različne sektorje in zagotavlja stalne preglede stanja kibernetske pripravljenosti (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

3.3 Vloga in pomen zakonodaje na področju kibernetske varnosti

Zakonodaja na področju kibernetske varnosti ni le orodje nadzora, temveč tudi pomemben instrument za izgradnjo zaupanja v digitalno družbo. Z jasno določenimi pravili se omogoča hitrejše ukrepanje ob incidentih, zmanjšuje pravna negotovost in spodbuja investicije v varnostno infrastrukturo. Za VOC zakonodaja predstavlja osnovo za organizacijo njihovega delovanja, oblikovanje notranjih pravilnikov, določitve postopkov in nadzor nad izvajanjem.

Med ključne prednosti zakonodajne urejenosti štejemo:

- formalizacijo procesov odzivanja in poročanja,
- boljšo usposobljenost kadra skozi standardizirane pristope,
- okrepljeno sodelovanje med javnim in zasebnim sektorjem,
- večje zaupanje uporabnikov in partnerjev.

Direktiva NIS 2 in ZInfV-1 tako ne le določata obveznosti, temveč tudi spodbujata razvoj kibernetske kulture in higiene. V prihodnosti lahko pričakujemo še dodatne akte, kot je Cyber Resilience Act, ki bo dodatno urejal kibernetsko varnost naprav in programske opreme v digitalni dobavni verigi.

Zato je pomembno, da VOC ne le sledijo zakonodaji, temveč jo tudi strateško vključijo v svojo dolgoročno vizijo. Na ta način lahko prispevajo k višji ravni digitalne odpornosti v Sloveniji in Evropi ter služijo kot zgled dobre prakse na področju varovanja informacijskih sistemov (Cybersecurity, 2024; Direktiva, 2022).

3.4 DORA in vloga VOC

Uredba EU 2022/2554 o digitalni operativni odpornosti za finančni sektor (DORA) je neposredno zavezujoč okvir EU, ki poenoti in nadgradi pravila upravljanja tveganj IKT v celotni finančni panogi. Njena logika je preprosta: finančne institucije morajo dokazljivo obvladovati celoten življenjski cikel kibernetskih tveganj – od preprečevanja in zaznavanja do odziva, okrevanja ter učenja – ob hkratnem nadzoru nad odvisnostjo od tretjih ponudnikov IKT (npr. gostovanje v oblaku). Kot posebni predpis DORA nadgrajuje direktivo NIS 2 na področju financ, kar se z ZInfV-1 odrazi tako, da se za bistvene in pomembne subjekte v bančništvu in finančni infrastrukturi uporabljajo neposredno pravila uredbe DORA, medtem ko se določena

poglavja ZInfV-1 ne uporabljajo (UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA, 2022).

Temelj uredbe DORA je okvir upravljanja tveganj IKT, ki zahteva jasne vloge upravljanja, politike in kontrole, procesno obravnavo incidentov ter zmožnost poročanja o večjih incidentih IKT po usklajeni evropski taksonomiji (izvedbene podrobnosti razvijajo evropski nadzorni organi EBA, ESMA in EIOPA). V praksi to pomeni, da morajo imeti finančni subjekti zmožnosti za spremljanje, zaznavanje in obravnavo incidentov, standardizirano dokumentacijo in sledljivost odločitev, in sicer tako za notranjo rabo kot za regulatorni nadzor (UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA, 2022).

Posebni steber uredbe DORA je digitalno preizkušanje odpornosti finančnih sektorjev. Organi določijo, kateri subjekti izvajajo napredne preizkuse TLPT (penetracijsko testiranje na podlagi analize groženj) najmanj vsaka tri leta. Preizkusi potekajo na aktivnih produkcijskih sistemih, zajeti pa morajo biti tudi deli, ki so zunanje oddani tretjim ponudnikom IKT. DORA predvideva tudi skupno TLP-testiranje, vzajemno priznavanje rezultatov in uradna potrdila o izvedbi v skladu z zahtevami (UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA, 2022).

Drugi ključni steber je upravljanje tveganj tretjih ponudnikov IKT. Za ključne ponudnike (npr. velike oblačne platforme) DORA vzpostavi evropski nadzorni okvir z glavnim nadzornikom in nadzorniškim forumom, ki ocenjujeta njihove kontrole (razpoložljivost, zaupnost, celovitost, neprekinjenost), obvladujeta koncentracijska tveganja in usklajujeta ukrepe na ravni Evropske unije. Finančni subjekti morajo pogodbeno in operativno zagotavljati nadzorljivost storitev, vključevati zahteve glede poročanja o incidentih ter imeti prehodne/izhodne strategije (UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA, 2022).

V tem okviru je VOC osrednji operativni mehanizem, s katerim finančne ustanove izpolnjujejo zahteve uredbe DORA. Zagotavlja neprekinjeno spremljanje, validacijo in klasifikacijo dogodkov, vodenje odziva, forenzično sledljivost in poročanje regulatorjem po zahtevanih postopkih. VOC sodeluje pri TLPT (priprava obsega, zagotavljanje dnevniških sledi, soočenje z rezultati) in tudi z ekipami za neprekinjeno poslovanje (BCP/DRP), da so RTO/RPO v praksi dosegljivi. Pri obvladovanju dobaviteljev VOC redno ocenjuje signale o razpoložljivosti in varnosti pri ključnih ponudnikih IKT, preverja izpolnjevanje pogodbenih SLA ter prispeva k skrbnim pregledom in revizijam. Vse to mora biti zajeto v politikah, postopkih in evidencah skladnosti, ki jih DORA zahteva in jih je treba redno testirati ter izpopolnjevati (UREDBA (EU)

2022/2554 EVROPSKEGA PARLAMENTA IN SVETA, 2022; Urad Vlade Republike Slovenije za informacijsko varnost, 2025).

4 UPRAVLJANJE TVEGANJ IN SODELOVANJE Z ZUNANJIMI DELEŽNIKI

V sodobnem digitalnem okolju, kjer se organizacije soočajo z vedno večjim številom kompleksnih kibernetskih groženj, je učinkovito upravljanje tveganj ključno za zagotavljanje neprekinjenega poslovanja, varstva informacijskih sredstev in skladnosti z regulativnimi zahtevami. To je še posebej pomembno za varnostno-operativne centre, katerih glavne naloge so pravočasno zaznavanje, preprečevanje, analiziranje in odzivanje na kibernetske dogodke. Zaradi dinamike groženj in hitrega razvoja tehnologij je nujno, da VOC vzdržujejo učinkovitost sistema obvladovanja tveganj, ki temelji na strukturiranih pristopih in aktivnem sodelovanju z zunanjimi deležniki. Tako sodelovanje vključuje nacionalne in mednarodne odzivne centre, regulatorne organe, ponudnike storitev ter ostale pomembne deležnike v ekosistemu kibernetske varnosti (Brown & Chase, 2020; ENISA, 2023a).

4.1 Upravljanje tveganj v varnostno-operativnem centru

Upravljanje tveganj v VOC obsega identifikacijo, oceno, obvladovanje in spremljanje tveganj, povezanih s kibernetsko varnostjo. VOC se pri tem procesu običajno opirajo na mednarodne standarde, kot sta ISO/IEC 27005:2018 in NIST Cybersecurity Framework (CFS) 2.0, ki zagotavljajo jasen in sistematičen pristop k obravnavi tveganj (ISO/IEC, 2018; NIST, 2024).

Prva faza pri upravljanju tveganj je identifikacija sredstev, ki jih je treba zaščititi, kar vključuje tako tehnične sisteme kot tudi podatke in procese. Temu sledi analiza groženj in ranljivosti, kjer VOC uporabljajo različne tehnike in vključujejo uporabo metrike, kot so verjetnost pojava incidenta, vpliv incidenta in ocena potencialne finančne škode (ENISA, 2023).

Za učinkovito spremljanje in zmanjševanje tveganj VOC uporabljajo različne tehnološke rešitve, kot so sistemi za upravljanje varnostnih informacij in dogodkov (SIEM), orodja za avtomatizacijo in orkestracijo odzivov (SOAR), rešitve za nadzor končnih točk oz. angl. *end-point protection* (EDR/XDR) ter sistemi za upravljanje ranljivosti (Brown & Chase, 2020).

Poleg tehničnih vidikov je bistvena tudi vloga človeškega dejavnika. Človeški faktor je nepogrešljiv pri interpretaciji varnostnih opozoril, odločanju v realnem času, strateškem usmerjanju ter v krizni komunikaciji znotraj in zunaj organizacije. Prav zato je vlaganje v izobraževanje analitikov in izgradnjo kulture kibernetske varnosti ključno za uspešno obvladovanje tveganj (Brown & Chase, 2020; ENISA; 2023b).

4.2 Sodelovanje z zunanjimi deležniki

Sodelovanje z zunanjimi deležniki je ključna komponenta učinkovitega delovanja varnostno-operativnih centrov. Zaradi vse večje kompleksnosti in globalizacije kibernetskih groženj postaja izolirano upravljanje kibernetske varnosti praktično nemogoče. Varnostni dogodki pogosto presegajo organizacijske, nacionalne ali celo sektorske meje, zato je učinkovito sodelovanje med različnimi deležniki nujno potrebno. Zunanji deležniki vključujejo širok spekter subjektov, kot so nacionalni odzivni centri, regulatorne agencije, mednarodne organizacije, specializirani ponudniki storitev, industrijska združenja in akademske institucije (ENISA, 2023a; Brown & Chase, 2020).

Pomembnost tega sodelovanja je še posebej poudarjena v kontekstu evropske direktive NIS 2 (Directive EU 2022/2555), ki izrecno zahteva vzpostavitev tesnejšega sodelovanja in učinkovitejšega pretoka informacij med organizacijami ter pristojnimi nacionalnimi in evropskimi organi. Prav tako standard ISO/IEC 27005 (2018) poudarja pomen interakcije z zunanjimi deležniki kot bistven za pravilno ocenjevanje in obvladovanje tveganj v organizacijskem okolju.

4.2.1 Nacionalni odzivni centri in regulatorni organi

Na nacionalni ravni VOC v Sloveniji aktivno sodelujejo s slovenskim nacionalnim odzivnim centrom za kibernetsko varnost. SI-CERT zagotavlja ključno operativno podporo s centralizirano zbirko podatkov o grožnjah, indikacijah kompromisa (IoC) in z usklajenim postopkom odzivanja na incidente. V praksi se sodelovanje pogosto izvaja preko neposrednih komunikacijskih kanalov, rednih poročil o varnostnih dogodkih in v okviru nacionalnih vaj kibernetske varnosti. Sodelovanje varnostno-operativnim centrom omogoča hitrejšo identifikacijo incidentov in ustreznejši odziv na grožnje, saj se lahko učinkovito odzivajo na najnovejše incidente in varnostne izzive v državi (SI-CERT, 2024).

Poleg centra SI-CERT pomembno vlogo igra tudi Agencija za komunikacijska omrežja in storitve Republike Slovenije (AKOS), ki nadzira skladnost s pravilnimi regulativami, predvsem z direktivo NIS 2. Redna komunikacija in poročanje tej agenciji zagotavljata pravočasno zaznavanje morebitnih neskladnosti ter pravočasen odziv na regulatorne spremembe (Europen Parliament & Council, 2022).

4.2.2 Evropske strukture sodelovanja: ENISA in mreža CSIRT

Na evropski ravni je osrednji akter Evropska agencija za kibernetsko varnost (ENISA), ki spodbuja sodelovanje prek mreže nacionalnih odzivnih centrov (CSIRT Network). ENISA organizira redne skupne vaje ter mednarodne simpozije in omogoča izmenjavo strateških ter taktičnih informacij o kibernetskih grožnjah (ENISA, 2023a). Skozi mrežo CSIRT organizacije iz različnih držav aktivno delijo indikatorje kompromisa, kar omogoča učinkovitejše prepoznavanje in blaženje širših, meddržavnih incidentov.

V okviru evropskega sodelovanja igra pomembno vlogo tudi mreža CyCLONe (Cyber Crisis Liaison Organization Network), ki služi kot operativna platforma za koordinacijo odziva na večje incidente z velikim vplivom na kritično infrastrukturo in nacionalno varnost posameznih držav članic. Sodelovanje z mrežo CyCLONe varnostno-operativnim centrom omogoča hiter dostop do informacij, ki jih delijo države članice v primeru kritičnih kibernetskih incidentov, ter usklajen odziv na dogodke, ki segajo preko nacionalnih meja (ENISA, 2023c).

4.2.3 Ponudniki varnostnih storitev (MSSP)

Zaradi omejenih virov, kadrovske podhranjenosti ali specifičnih zahtev, povezanih s kompleksnostjo groženj, se organizacije pogosto odločajo za sodelovanje s ponudniki upravljanih varnostnih storitev (Managed Security Service Provider – MSSP). Takšno sodelovanje varnostno-operativnim centrom omogoča razširitev operativnih zmogljivosti, izboljšanje odzivnosti in dostop do specializiranega znanja ter tehnologij, ki jih znotraj organizacije ne posedujejo.

Sodelovanje z MSSP poteka preko natančno opredeljenih pogodb, ki vsebujejo jasno določene nivoje storitev (Service Level Agreements – SLA), odzivne čase, postopke poročanja in zahteve glede skladnosti z zakonodajo, zlasti z direktivo NIS 2 (European Parliament & Council, 2022). S tem se zagotavlja, da je kakovost varnostnih storitev ustrezna, odzivi hitri in da se tveganja glede zunanjega izvajanja ustrezno upravljajo.

4.2.4 Industrijska združenja in akademska skupnost

VOC aktivno sodelujejo tudi z industrijskimi združenji, kot so centri ISAC (Information Sharing and Analysis Centers). Ta združenja omogočajo sistematično izmenjavo podatkov o specifičnih grožnjah znotraj posameznih sektorjev, kot so na primer finančni, energetski in zdravstveni sektor. Takšno sodelovanje pomembno povečuje zavedanje o specifičnih grožnjah in omogoča hitrejšo odzivnost VOC na sektorsko specifične kibernetske incidente (ENISA, 2023b).

Sodelovanje z akademsko skupnostjo prav tako prinaša pomembne prednosti, kot so dostop do najnovejših raziskav na področju kibernetske varnosti, razvoj novih tehnologij za zaznavanje in preprečevanje groženj ter možnosti za izobraževanje in usposabljanje kadrov. Številni VOC v Sloveniji in Evropi vzpostavljajo tesne odnose z univerzami in raziskovalnimi inštituti, kar jim omogoča nenehen razvoj in izboljšanje operativnih postopkov ter tehnoloških rešitev.

5 VARNOSTNO-OPERATIVNI CENTRI V SLOVENSKEM PROSTORU

Varnostno-operativni centri so ključni del varnostne infrastrukture vsake sodobne organizacije, saj zagotavljajo sistematičen pristop k odkrivanju, analizi, preprečevanju in odzivanju na kibernetske grožnje. V slovenskem prostoru postajajo bolj razširjeni predvsem zaradi naraščajoče kompleksnosti kibernetskih dogodkov, novih regulativnih zahtev Evropske unije, kot je direktiva NIS 2, in vse večje potrebe po učinkoviti zaščiti kritične infrastrukture. Pričujoče poglavje analizira trenutno stanje VOC v Sloveniji, strukturo njihovega delovanja, posebnosti nacionalnega pristopa in izzive, s katerimi se srečujejo v svojem delovanju.

5.1 Struktura in organiziranost VOC v Sloveniji

Slovenski VOC so praviloma organizirani po večstopenjski strukturi, ki jo sestavljajo različni nivoji analitikov in vodstvo. Ta struktura omogoča jasno porazdelitev odgovornosti, učinkovit odziv na incidente in ustrezno upravljanje virov ter kompetenc znotraj centra.

Analitiki nivoja 1 predstavljajo začetno stopnjo odziva, kjer se opravljajo osnovna diagnostika dogodkov, spremljanje sistemov in začetno preverjanje indikatorjev ogroženosti sistema. Analitiki nivoja 2 zagotavljajo podrobnejšo analizo varnostnih incidentov, raziskovanje kompleksnejših dogodkov in koordinacijo odziva na resnejše grožnje. Analitiki nivoja 3 so običajno visoko specializirani strokovnjaki, ki opravljajo najzahtevnejše kibernetske napade, digitalne forenzične preiskave in odkrivanje naprednih groženj ter sodelujejo pri izboljševanju tehnoloških rešitev in metodologij centra (ENISA Threat Landscape, 2023).

5.2 Struktura VOC glede na velikost organizacije

V Sloveniji se struktura in delovanje VOC bistveno razlikujeta glede na velikost organizacije in sektorja, v katerem ta deluje. Razlikujemo tri osnovne tipe VOC glede na njihovo velikost. Pri opredelitvi velikosti organizacije se v Sloveniji praviloma upoštevajo število zaposlenih, letni prihodek in kompleksnost IT-infrastrukture. Glede na te dejavnike ločimo tri kategorije: velike, srednje velike in majhne organizacije (Kajdiž, 2024).

5.2.1 VOC v velikih organizacijah

Velike organizacije v Sloveniji so praviloma tiste, ki imajo več kot 250 zaposlenih, letni prihodek, ki presega 50 milijonov evrov, ter kompleksno IT-infrastrukturo, pogosto razširjeno na več lokacij, tudi izven Slovenije (Kajdiž, 2024; Zakon o gospodarskih družbah (ZGD-1)). V to skupino običajno spadajo banke, velike telekomunikacijske družbe, energetska podjetja ter večje državne institucije, pa tudi velika podjetja, ki se ukvarjajo s proizvodnjo in trgovino. V proizvodnih in trgovskih podjetjih je organiziranost pogosto manj centralizirana, varnostne funkcije so lahko del širšega IT-oddelka, medtem ko je VOC zunanji partner.

VOC v velikih organizacijah delujejo kontinuirano – 24 ur na dan, vseh sedem dni v tednu. Njihova struktura je kompleksna in jasno hierarhično organizirana, vključuje več ravni analitikov (nivo 1, nivo 2, nivo 3) in ima posebej določeno vodstveno ekipo za strateško upravljanje. VOC v velikih podjetjih pogosto vključuje:

- **specializirane analitike nivoja 1**, ki izvajajo začetno spremljanje varnostnih dogodkov;
- **analitike nivoja 2**, ki so odgovorni za globljo analizo incidentov, izvajanje odzivnih postopkov in koordinacijo ukrepov;
- **visoko specializirane analitike nivoja 3**, ki se ukvarjajo z napredno analizo groženj, digitalno forenzično preiskavo incidentov in sodelovanjem pri razvoju varnostnih strategij ter rešitev;
- **varnostne vodje in menedžerje**, ki nadzorujejo splošno delovanje, zagotavljajo skladnost z zakonodajnimi zahtevami, kot je direktiva NIS 2, in skrbijo za upravljanje odnosov z zunanjimi deležniki.

Za podporo svojemu delu ti centri uporabljajo napredne tehnološke rešitve, kot so SIEM, EDR/XDR, SOAR, in različne platforme za obveščanje o grožnjah (angl. *threat intelligence*). Prav tako so pogosto vključeni v širše mednarodne mreže za izmenjavo informacij o grožnjah.

5.2.2 VOC v srednje velikih organizacijah

Srednje velike organizacije v Sloveniji imajo običajno od 50 do 250 zaposlenih in letni prihodek, ki ne presega 50 milijonov evrov, vendar je višji od 10 milijonov evrov. Njihova infrastruktura je manj kompleksna kot pri velikih organizacijah, a še vedno dovolj obsežna, da

potrebuje namenski varnostni nadzor (Kajdiž, 2024; Zakon o gospodarskih družbah, 2006). V to kategorijo pogosto sodijo srednje velika proizvodna podjetja, trgovske verige, večja IT-podjetja in določene javne ustanove.

VOC srednje velikih organizacij praviloma nimajo kontinuiranega delovanja, ampak obratujejo po prilagojenem urniku, ki ga narekuje poslovni delovni čas, občasno pa gre tudi za spremljanje izven tega časa. Njihova organizacija običajno vključuje manj analitikov, ti pa pogosto opravljajo več nalog hkrati. To pomeni, da en človek dela na nivojih 1 in 2, medtem ko kompleksnejše preiskave pogosto izvajajo zunanji izvajalci oziroma ponudniki MSSP (na nivoju 3). Za varnostno spremljanje uporabljajo osnovne rešitve, kot sta SIEM in EDR, delno pa uporabljajo tudi rešitve za avtomatizacijo odziva SOAR, vendar v precej omejenem obsegu. Če ima podjetje, ki se ukvarja z dejavnostjo, kot je gostovanje, klicni center, ki neprestano deluje, se del nalog z nivoja 1 preseli v klicni center (ENISA, Good practices for supply chain cybersecurity, 2023). Velikokrat pa podjetja, ki imajo svoj VOC, ne pa tudi dovolj kadrov, VOC združijo s pogodbo o opravljanju nivojev 1 in 2 izven poslovnega delovnega časa.

5.2.3 VOC v majhnih organizacijah

Majhne organizacije so opredeljene kot podjetja, ki imajo manj kot 50 zaposlenih, njihov letni prihodek pa ne presega 10 milijonov evrov. Te organizacije imajo omejene vire in praviloma zelo preprosto IT-infrastrukturo (Kajdiž, 2024; Zakon o gospodarskih družbah, 2006). V to skupino sodijo manjša podjetja, mikropodjetja, manjše storitvene dejavnosti in podobno.

Večina majhnih slovenskih organizacij nima internega VOC, ampak varnostne funkcije popolnoma ali skoraj v celoti zunanje izvajajo preko specializiranih ponudnikov varnostnih storitev (MSSP). Sodelovanje z MSSP jim omogoča, da kljub omejenim notranjim virom zagotovijo zadostno raven varnostnega nadzora, skladnost z regulativo, kot je NIS 2, in hitro odzivanje v primeru varnostnih incidentov. Notranja ekipa, če sploh obstaja, je običajno zelo majhna in se osredotoča predvsem na koordinacijo z zunanjimi izvajalci ter osnovno interno samoozaveščanje o varnostnih tveganjih (SI-CERT, 2024).

5.3 Primer dobrih praks v Sloveniji

Primeri dobre prakse delovanja VOC v Sloveniji vključujejo predvsem organizacije iz finančnega, energetskega, telekomunikacijskega in javnega sektorja, ki so zaradi visoke stopnje tveganj med prvimi vzpostavile napredne VOC.

Med vidnejšimi primeri je CKVO (Center kibernetske varnosti in odpornosti) v okviru Telekoma Slovenije, ki deluje skladno z mednarodnimi standardi, kot so ISO/IEC 27001, ISO/IEC 27005 in NIST CSF. Ta center izvaja kontinuirano spremljanje omrežja in preventivne varnostne ukrepe ter redno sodeluje z nacionalnimi in mednarodnimi institucijami pri izmenjavi informacij o grožnjah (Slovenija).

Podoben pristop k zagotavljanju kibernetske varnosti uporablja tudi podjetje Unistar LC, d. o. o., ki je razvilo napreden varnostno-operativni center (SOC), imenovan PRO.SOC. Ta center deluje kot osrednji živčni sistem za zaznavanje, analizo in odzivanje na kibernetske grožnje, pri čemer uporablja eno izmed najzanesljivejših SIEM-platform na trgu: IBM QRadar. Platforma omogoča zbiranje in analizo varnostnih dogodkov iz različnih virov, kot so oblačne storitve, končne točke, aplikacije, omrežja in strežniki, ter zagotavlja jasen kontekst za razumevanje resnosti tveganj. Poleg tega Unistar LC v VOC vključuje tudi lastno rešitev, in sicer Chaty AI – digitalnega pomočnika, ki z uporabo umetne inteligence avtomatizira razvrščanje dogodkov, prepoznava vzorce in filtrira lažne alarme. To omogoča hitrejši odzivni čas in analitikom omogoča, da se osredotočijo na primere, kjer je človeška prisotnost ključna. Unistar LC ponuja tudi storitve SOC-as-a-Service (SOCaaS), ki podjetjem vseh velikosti omogočajo dostop do naprednih varnostnih storitev brez potrebe po lastni infrastrukturi. Ta naročniški model zagotavlja vse prednosti namenskega lastnega neprekinjenega VOC, vendar brez visokih stroškov in kompleksnosti, ki jih prinašata izgradnja in upravljanje VOC v podjetju. S tem pristopom Unistar LC podjetjem omogoča, da izboljšajo svojo kibernetsko varnost, zmanjšajo tveganja in se učinkovito odzivajo na grožnje, ne glede na velikost ali panogo, v kateri podjetje ali organizacija deluje.

5.4 Izzivi VOC v Sloveniji

Kljub pozitivnim primerom se slovenski VOC soočajo s številnimi izzivi, med katerimi so najpogostejši pomanjkanje kvalificiranih kadrov, omejene finančne zmožnosti za vzpostavitev napredne infrastrukture in nizka stopnja ozaveščenosti organizacij glede pomembnosti vlaganja v kibernetsko varnost (SI-CERT, 2024).

Pomanjkanje strokovnih kadrov je eden najresnejših izzivov, ki ga potrjujejo redne raziskave in poročila centra SI-CERT ter agencije ENISA. Slovenske organizacije težko tekmujejo z drugimi evropskimi državami pri privabljanju vrhunskih strokovnjakov, kar posledično vpliva na sposobnost hitrega odzivanja in učinkovitega preprečevanja kompleksnih kibernetskih incidentov (ENISA Threat Landscape, 2023).

Dodatno težavo predstavlja razdrobljenost pristopa h kibernetski varnosti, ker nekatere organizacije še vedno delujejo brez jasno strukturiranega VOC in posledično niso sposobne učinkovito zaznati in se odzvati na sodobne kibernetske grožnje.

5.5 Skladnost z direktivo NIS 2

S sprejetjem direktive NIS 2 so slovenske organizacije dodatno obvezane k vzpostavitvi ali nadgradnji varnostno-operativnih centrov. Direktiva NIS 2 organizacijam nalaga jasno določene zahteve glede upravljanja tveganj, poročanja incidentov in sodelovanja z nacionalnimi organi. Slovenski VOC so tako zavezani k pravočasni in strukturirani prijavi incidentov, rednemu izvajanju vaj in simulacij ter tesnemu sodelovanju z nacionalnimi regulatornimi organi (Direktiva 2022/2555, 2022).

Prilagajanje tem zahtevam predstavlja dodaten pritisk na slovenske organizacije, a hkrati priložnost za krepitev odpornosti in izboljšanje operativne pripravljenosti VOC.

V kontekstu slovenskega prostora to pomeni, da so organizacije v določenih ključnih in pomembnih sektorjih, kot so energetika, promet, zdravstvo, digitalna infrastruktura, bančništvo in javna uprava, neposredno zavezane k vzpostavitvi ali nadgradnji VOC. Ti imajo ključno vlogo pri zagotavljanju skladnosti z določbami direktive, saj omogočajo centralizirano upravljanje tveganj, zaznavanje in odzivanje na incidente, dokumentiranje ter obveščanje pristojnih organov.

Med ključnimi zahtevami direktive, ki vplivajo na delovanje VOC, so:

- ***Vzpostavitev sistemov za obvladovanje kibernetskih tveganj***, ki vključujejo tehnične in organizacijske ukrepe.
- ***Obveznost poročanja incidentov***: organizacije morajo resne incidente prijaviti v 24 urah, dodatno poročilo pripraviti v 72 urah in zaključno oceno v enem mesecu od incidenta. VOC morajo zato zagotavljati učinkovite postopke zaznavanja, evidentiranja in eskalacije incidentov (Direktiva 2022/2555, 2022).

- ***Izvajanje rednih vaj in testiranje***: VOC morajo sodelovati v nacionalnih in medsektorskih vajah, ki jih koordinirajo SI-CERT, CyCLONe ali ENISA. To vključuje tako tehnične simulacije kot tudi operativno-komunikacijske vaje.
- ***Ocenjevanje dobaviteljev in tretjih strani***, kar pomeni, da VOC vključijo spremljanje tveganj v dobavni verigi kot del svojega rednega operativnega nadzora.
- ***Zagotavljanje usposobljenosti osebja***, vključno z rednimi programi izobraževanja in izpopolnjevanja, zlasti na ravni analitikov in upravljavcev tveganj.

Slovenski VOC so v zadnjih letih že začeli prilagajati svoje delovanje novim zahtevam. Večina večjih organizacij, zlasti v sektorjih, ki jih direktiva neposredno zadeva, je okrepila kapacitete, nadgradila orodja za zaznavanje in odzivanje ter vzpostavila stalne kontakte s centrom SI-CERT in pristojnimi ministrstvi.

Prilagajanje tem zahtevam sicer predstavlja dodaten organizacijski, kadrovski in finančni pritisk, vendar prinaša tudi dolgoročne koristi. Vključevanje standardiziranih praks upravljanja varnosti in testiranja odzivnih zmogljivosti prispeva k večji odpornosti, zmanjšanju časa zaznave in hitrejšemu okrevanju po incidentih. Prav tako vzpostavlja temelje za večje zaupanje med deležniki, vključno s strankami, regulatorji in partnerji v dobavni verigi.

NIS 2 pomeni tudi dvig odgovornosti vodstvenih struktur, saj so v direktivi prvič jasno opredeljene obveznosti in sankcije za vodstva organizacij, ki ne zagotovijo ustrezne ravni kibernetske varnosti. Tako se vloga vodstva VOC povečuje ne le z vidika operativnega nadzora, temveč tudi z vidika strateškega upravljanja tveganj in pravne odgovornosti. Na zakonodajni ravni se v Sloveniji pričakuje prenos direktive v nacionalni pravni red do konca leta 2024/25, kar bo pomenilo še večjo pravno obveznost organizacij za vzpostavitev ustrezne strukture VOC ter za učinkovito upravljanje kibernetske varnosti.

5.6 Prihodnji razvoj VOC v Sloveniji

Prihodnji razvoj varnostno-operativnih centrov (VOC) v slovenskem prostoru bo zaznamovan z več ključnimi strateškimi usmeritvami, ki izhajajo tako iz potreb po večji odpornosti proti kibernetskim grožnjam kot iz regulatornih zahtev in tehnoloških inovacij. Med najbolj izpostavljenimi trendi so avtomatizacija, uporaba umetne inteligence, okrepljeno sodelovanje z zunanjimi deležniki ter sistematična integracija akademskega in raziskovalnega znanja v delovanje VOC.

5.6.1 Avtomatizacija in orkestracija odziva

Zaradi pomanjkanja kadra in naraščajoče količine varnostnih dogodkov bodo VOC v prihodnje še intenzivneje vlagali v avtomatizacijo zaznave in odziva s poudarkom na:

- ***SOAR-platformah (Security Orchestration, Automation and Response)***, ki omogočajo integracijo različnih orodij, kot so SIEM, EDR in *threat intelligence*, ter avtomatizacijo standardnih odzivnih protokolov, kot so blokiranje IP-naslova, izolacija naprav in eskalacija incidenta.
- ***Avtomatizaciji Runbook***, kjer bodo vsakodnevni postopki, kot so lažni alarmi, osnovne poizvedbe ter preverjanje IoC, formalizirani in izvedeni brez človeškega posredovanja.
- ***Avtomatiziranem poročanju*** regulatornim organom v skladu z direktivo NIS 2, kjer bodo iz vnaprej definiranih kriterijev in predlog poročila samodejno generirala obvestila za SI-CERT in upravne organe.

Cilj avtomatizacije je zmanjšanje tako imenovanega pojava *analyst fatigue* in povečanje učinkovitosti VOC, kjer bodo človeški viri osredotočeni na odločanje, strategijo in analizo kompleksnih groženj.

5.6.2 Umetna inteligenca in strojno učenje

VOC bodo v prihodnosti vse bolj uporabljali napredne algoritme umetne inteligence (AI) in strojnega učenja predvsem za:

- ***analizo anomalij in vedenjskih vzorcev*** v omrežjih, kot je na primer UEBA – User and Entity Behavior Analytics;
- ***predikativno analitiko***, kjer sistem na osnovi preteklih dogodkov napove možne prihodnje incidente;
- ***filtriranje lažnih pozitivnih alarmov***, kar je ključnega pomena pri zmanjšanju operativne preobremenjenosti analitikov.

V Sloveniji že obstajajo prvi primeri vključevanja lokalno razvitih AI-pomočnikov, kot je na primer Chaty AI v okviru Unistar LC, kar kaže na potencial domačega znanja za razvoj specializiranih rešitev za VOC (Unistar LC, d. o. o., 2025).

5.6.3 Kibernetska suverenost in sodelovanje

Zaradi geopolitičnih tveganj in večje osredotočenosti EU na digitalno suverenost se bo povečal poudarek na notranjem razvoju zmogljivosti VOC v Sloveniji in s tem zmanjševanju odvisnosti od zunanjih tehnologij, ki niso evropskega porekla, ter oblikovanju regionalnih centrov sodelovanja.

Slovenija bo verjetno sledila pobudam, kot so:

- modeli EU SOC-as-a-Service, ki jih spodbujajo ENISA, ECSO in Horizon Europa;
- vzpostavitev nacionalnih skupnih operativnih centrov za specifične sektorje;
- okrepljeno sodelovanje v pobudah, kot je CSIRT Network ali EU CyCLONe, kjer bodo nacionalni VOC igrali operativno in strateško vlogo pri odzivanju na čezmejne incidente.

5.6.4 Sodelovanje z akademsko in raziskovalno sfero

Prihodnost razvoja VOC bo v veliki meri odvisna od vključevanja znanstveno-raziskovalne skupnosti, ki lahko prispeva k razvoju:

- novih algoritmov zaznave napadov in prepoznavanja TTP (Tactics, Techniques and Procedures);
- simulacijskih okolij za vaje, ki omogočajo realistično testiranje odzivnih zmogljivosti;
- izobraževalnih programov za analitike, ki bodo pokrivali tako tehnične kot upravljavske vidike delovanja VOC.

Potrebna bo tudi večja vključenost študentov in diplomantov tehniških in varnostnih programov v delovanje VOC, bodisi preko praks in projektov ali v okviru interdisciplinarnih raziskovalnih skupin.

5.6.5 Personalizacija in modularna arhitektura VOC

V prihodnosti bodo VOC bolj modularno strukturirani, kar pomeni, da bo možno prilagoditi arhitekturo centra glede na velikost, sektor in stopnjo tveganja organizacije. Modularni pristop omogoča:

- hibridne modele delovanja, na primer lastni VOC in podpora MSSP;
- porazdeljene analitične zmogljivosti, kjer se del nadzora izvaja lokalno, del pa centralizirano;
- skalabilnost, kar omogoča prilagajanje obsega storitev glede na razvoj groženj in poslovno rast (univ. dipl. inž. rač. in inf. Marko Zavadlav, osebna komunikacija, julij 2025).

6 VARNOSTNO-OPERATIVNI CENTRI V EVROPSKEM PROSTORU

V evropskem prostoru so varnostno-operativni centri ključna obrambna točka organizacij pri preprečevanju in obvladovanju kibernetskih groženj. Evropski VOC predstavljajo sodobno prakso varovanja informacijskih sistemov in kritične infrastrukture ter so ključnega pomena za ohranjanje visoke ravni kibernetske varnosti v državah Evropske unije. Pri analizi najboljših praks evropskih VOC izpostavljamo predvsem pristop, ki kombinira visokotehnološko avtomatizacijo in poudarek na človeškem faktorju kot ključni komponenti sodobne kibernetske zaščite (Kathryn Knerler, 2024).

6.1 Najboljše evropske prakse VOC

Evropski VOC delujejo skladno s standardiziranimi smernicami, kot so tiste, izpostavljene v direktivi NIS 2 in standardu ISO/IEC 27001, ter sledijo praksam, ki omogočajo učinkovito zaznavanje, analizo in odzivanje na varnostne incidente (Direktiva 2022/2555, 2022).

Med vodilne evropske prakse sodijo:

1. ***Integracija kibernetske obveščevalne dejavnosti***: evropski VOC uporabljajo napredne platforme za kibernetsko obveščanje, kot so Threat Intelligence Platforms ali TIP, ki omogočajo zbiranje, analizo in distribucijo varnostnih informacij med analitiki na VOC in drugimi zainteresiranimi deležniki. To omogoča hitrejšo reakcijo na incidente in boljšo pripravljenost na prihodnje grožnje (Kathryn Knerler, 2024).
2. ***Proaktivno iskanje groženj (Threat Hunting)***: namesto zgolj pasivnega odzivanja na zaznane incidente napredni evropski VOC aktivno iščejo potencialne grožnje v svojih omrežjih. Z uporabo tehnik napredne analitike, strojnega učenja in profiliranja uporabniškega vedenja analitiki na VOC prepoznavajo vzorce in anomalije, ki bi lahko nakazovale potencialne kibernetske incidente (Kathryn Knerler, 2024).
3. ***Široka uporaba avtomatizacije in orodij SOAR***: evropski VOC implementirajo orodja Security Orchestration Automation and Response ali SOAR, ki avtomatizirajo rutinske postopke, kot sta osnovna analiza incidentov in obogatitev podatkov o grožnjah, ter enostavne odzivne ukrepe, kar omogoča hitrejše reakcije na incidente in zmanjšuje tveganje za človeške napake (Kathryn Knerler, 2024).

4. ***Zavezanost standardom skladnosti***: VOC v Evropi so močno osredotočeni na izpolnjevanje zahtev evropske zakonodaje, kot sta direktiva NIS 2 in GDPR, kar zagotavlja visoke standarde informacijske varnosti in zasebnosti. To vključuje sistematično upravljanje tveganj in poročanje o incidentih skladno z regulatornimi zahtevami.

6.2 Avtomatizacija v evropskih VOC

Avtomatizacija je postala eden ključnih stebrov učinkovitosti evropskih VOC. Omogoča zmanjšanje odzivnih časov in optimizacijo človeških virov. Evropski VOC pogosto uporabljajo orodja za avtomatsko zaznavanje, klasifikacijo in prioritizacijo incidentov. Takšna avtomatizacija vključuje:

- avtomatizirano zaznavanje in klasifikacijo incidentov,
- avtomatizirane odzivne ukrepe, kot sta izolacija okuženih naprav in blokiranje sumljivih IP-naslovov,
- avtomatizirano zbiranje in obogatitev informacij o incidentih z uporabo kibernetske inteligence (Kathryn Knerler, 2024).

Najnaprednejši VOC v Evropi avtomatizirajo tudi kompleksne odzivne postopke, kar vključuje povezavo z orodji SIEM za natančno in hitro korelacijo dogodkov v realnem času (Scapicchio, Downie & Finio, 2024).

6.3 Pomen človeškega faktorja v evropskih VOC

Kljub intenzivni avtomatizaciji ostaja človeški faktor eden izmed nepogrešljivih elementov okolij v VOC. Evropski VOC zato veliko vlagajo v razvoj usposobljenosti svojih analitikov, ki so sposobni interpretirati kompleksne podatke, kritično razmišljati in sprejemati ključne odločitve pri odzivanju na incidente. Pomen človeškega dejavnika je ključen predvsem v naslednjih vidikih:

- sposobnost razumevanja konteksta incidentov in njihovega vpliva na poslovne procese,
- izvajanje kompleksnih analiz, ki jih avtomatizacija ne zmore učinkovito opraviti,
- inovativnost in prilagodljivost pri odzivanju na nove in nepoznane grožnje,
- zagotavljanje komunikacije z notranjimi in zunanjimi deležniki ter regulativnimi organi (Kathryn Knerler, 2024).

Prav tako je pomembno stalno izobraževanje in usposabljanje analitikov, s čimer VOC zagotavljajo pripravljenost na hitre spremembe v okolju kibernetskih groženj (ENISA, Report on the State of the Cybersecurity in the Union, 2024).

6.4 Delovanje varnostno-operativnih centrov v evropskem prostoru

VOC v evropskem prostoru predstavljajo eno ključnih struktur, ki organizacijam omogoča učinkovito upravljanje, odkrivanje, preprečevanje in odzivanje na kibernetske grožnje. Njihova primarna naloga je zagotavljanje visoke ravni kibernetske varnosti z uporabo naprednih tehnologij in procesov, ob tem pa so pomembno osredotočeni tudi na človeške vire in njihove kompetence (Kathryn Knerler, 2024).

VOC v Evropi delujejo skladno s smernicami Evropske unije, še posebej z direktivo NIS 2, ki opredeljuje temeljne zahteve glede organiziranosti in obveznosti na področju kibernetske varnosti. Njegovo delovanje je tipično organizirano v jasno strukturirane ravni, ki omogočajo učinkovito izvajanje nalog.

Proces delovanja VOC v evropskem prostoru zajema naslednje ključne aktivnosti:

1. ***Spremljanje oz. monitoring***: evropski VOC izvajajo neprekinjeno spremljanje informacijskih sistemov vse dni v letu s pomočjo naprednih orodij, kot so sistemi SIEM in različni sistemi za zaznavanje vdorov, kot je IDS (Intrusion Detection Systems). To jim omogoča hitro zaznavanje potencialnih incidentov, kar je ključno za takojšen odziv (Kathryn Knerler, 2024).
2. ***Zaznavanje incidentov oz. detection***: VOC uporabljajo avtomatizirane sisteme in strojno učenje za zgodnje odkrivanje anomalij v omrežju. To vključuje odkrivanje neobičajnih vzorcev, zlorab, ranljivosti in poskusov vdora v sistem. Evropski VOC so pogosto opremljeni z najsodobnejšimi orodji, kot so orodja SOAR, ki avtomatizirajo številne procese zaznavanja in odzivanja (Scapicchio et al., 2024).
3. ***Analiza incidentov oz. analysis***: analiza incidentov poteka v več fazah. Na prvi stopnji analitiki nivoja 1 hitro razvrstijo incidente glede na pomembnost in grožnjo, nato pa jih usmerijo na poglobljeno analizo v višjih stopnjah – na nivojih 2 in 3. Poglobljena analiza vključuje digitalno forenziko, analizo zlonamerne programske opreme in identificiranje vzrokov incidentov. Analitiki pri tem uporabljajo specializirana orodja za forenziko in napredno analitiko (Kathryn Knerler et al., 2024).

4. ***Odzivanje na incident oz. incident response***: v primeru potrjenega incidenta VOC aktivira vnaprej določene odzivne protokole. Odzivni postopki vključujejo omejitev škode, izolacijo prizadetih sistemov, obveščanje pristojnih organov in drugih deležnikov ter sprožitev ukrepov za zmanjšanje verjetnosti ponovitve incidenta. Evropski VOC pri odzivanju na incidente pogosto sodelujejo z nacionalnimi organi za kibernetsko varnost, kot so CERT, nacionalni CSIRT in Evropska agencija za kibernetsko varnost – ENISA (Direktiva 2022/2555, 2022).
5. ***Dokumentacija in poročanje oz. reporting***: evropski VOC so obvezani dokumentirati vse pomembne informacije o incidentih in redno poročati pristojnim organom skladno z direktivo NIS 2 ter drugimi regulativnimi zahtevami. Takšna dokumentacija omogoča transparentnost postopkov in vzdrževanje visokih standardov kibernetske varnosti (Direktiva 2022/2555, 2022).
6. ***Proaktivno iskanje groženj oz. threat hunting***: napredni evropski VOC ne delujejo zgolj reaktivno, ampak se ukvarjajo s proaktivnim iskanjem morebitnih groženj v omrežju. S takšnimi praksami, ki vključujejo specializirane tehnike analize podatkov in vzorcev, prehitevajo potencialne grožnje, preden te povzročijo resne posledice (Kathryn Knerler, 2024).
7. ***Kontinuirano izboljševanje in usposabljanje***: delovanje VOC v Evropi temelji tudi na stalnem izboljševanju in prilagajanju varnostnih procesov glede na najnovejše kibernetske grožnje in trende. VOC nenehno vlagajo v izobraževanje in usposabljanje analitikov, kar omogoča nenehno prilagodljivost in visoko raven pripravljenosti (Cybersecurity, 2024).

6.5 Velikost varnostno-operativnih centrov v Evropi in njihova povezanost s številom IP-naslovov

V evropskem prostoru se velikost in obseg delovanja varnostno-operativnih centrov razlikujeta glede na več ključnih dejavnikov, kot so vrsta organizacije, stopnja kibernetskih tveganj, razpoložljivi viri in predvsem kompleksnost ter velikost informacijskega omrežja podjetja. Pri slednjem je pomemben dejavnik prav število IP-naslovov, ki jih organizacija upravlja, saj to neposredno vpliva na obseg potrebnega spremljanja analize in odzivanja na incidente (Kathryn Knerler, 2024).

6.5.1 Velikost VOC v Evropi

VOC v Evropi se običajno delijo na tri glavne kategorije glede na velikost in število zaposlenih analitikov:

- ***Majhni VOC***: ti imajo običajno od 2 do 10 analitikov, pogosti so v manjših podjetjih, ki upravljajo manjše informacijske sisteme z relativno nizkim številom IP-naslovov. Zaradi manjšega obsega je pogosto mogoče obvladovati tveganja tudi z manjšo skupino ter uporabo osnovnih sistemov za spremljanje in analizo dogodkov (Kathryn Knerler, 2024).
- ***Srednje veliki VOC***: v srednje velikih VOC je zaposlenih od 10 do približno 50 analitikov in so pogosti tako v srednje velikih in večjih podjetjih kot tudi v večini javnih institucij. Te organizacije pogosto upravljajo večje število IP-naslovov, kar pomeni tudi kompleksnejše spremljanje in širši obseg aktivnosti, vključno s poglobljenimi analizami incidentov, proaktivnim iskanjem groženj ter uporabo naprednejših orodij (Cybersecurity, 2024).
- ***Veliki VOC***: največji evropski VOC običajno zaposlujejo več kot 50 analitikov, kar je značilno za velike multinacionalke, velike javne ustanove, ponudnike kritične infrastrukture in državne institucije, kot so nacionalni CSIRT. Ti VOC praviloma upravljajo zelo obsežna omrežja s tisoči IP-naslovov, ki zahtevajo močno specializirane ekipe ter zelo razvito infrastrukturo in visoko stopnjo avtomatizacije (Kathryn Knerler, 2024).

6.5.2 Povezanost velikosti VOC s številom IP-naslovov v podjetju

Število IP-naslovov, ki jih upravlja podjetje, neposredno vpliva na zahtevnost spremljanja in obvladovanja kibernetskih groženj. Večje število IP-naslovov običajno pomeni večjo izpostavljenost kibernetskim tveganjem ter višjo stopnjo kompleksnosti spremljanja in odzivanja (Kathryn Knerler, 2024).

- ***Majhna podjetja (manj kot 500 IP-naslovov)***: podjetja z manjšim številom IP-naslovov pogosto ne potrebujejo obsežnega VOC, saj je mogoče učinkovito obvladovati spremljanje tudi z majhno ekipo ali celo zunanjimi ponudniki storitev. V takšnih okoljih se pogosto uporabljajo osnovni sistemi SIEM in minimalna avtomatizacija (Kathryn Knerler, 2024).
- ***Srednje velika podjetja (od 500 do 5000 IP-naslovov)***: podjetja z večjim številom IP-naslovov potrebujejo strukturiran VOC, saj so zahtevani obsežnejše spremljanje, večja analitska moč ter pogostejša uporaba naprednih orodij, kot so sistemi za avtomatizirano

upravljanje odziva SOAR, in aktivna uporaba kibernetske obveščevalne dejavnosti. V teh primerih je pogost pristop segmentacija omrežij, ki omogoča lažje spremljanje in učinkovitejše odzivanje.

- ***Velika podjetja in organizacije (več kot 5000 IP-naslovov)***: organizacije s tisoči IP-naslovov se soočajo z izjemno kompleksnimi izzivi spremljanja in odzivanja. V teh primerih je velikost VOC praviloma največja, vključuje visoko specializirane ekipe ter uporabo obsežnih orodij za avtomatizacijo in analitiko. Omrežja teh organizacij so praviloma jasno segmentirana glede na poslovne funkcije, geografske lokacije ali kritične sisteme, kar omogoča boljše upravljanje in odzivanje na grožnje (Kathryn Knerler, 2024).

6.5.3 Delitev VOC glede na segmentacijo IP-naslovov

Segmentacija IP-naslovov oziroma omrežij je običajna praksa evropskih VOC. Ta praksa omogoča učinkovitejše spremljanje, analizo in odzivanje na grožnje, predvsem v večjih organizacijah. Delitev se običajno izvaja glede na:

- ***Poslovne funkcije***: gre za specifične segmente, kot so finance, kadrovski oddelki, razvojni oddelek in IT-infrastruktura.
- ***Stopnjo kritičnosti***: ločeni so segmenti za kritične sisteme in občutljive podatke.
- ***Geografsko lokacijo***: gre za segmente omrežij glede na fizične lokacije podjetja, kar omogoča jasno določitev odgovornosti posameznih analitikov na VOC (Kathryn Knerler, 2024).

Takšna segmentacija bistveno poveča učinkovitost odzivanja VOC, zmanjša čas zaznavanja in obravnave incidentov ter poveča splošno varnost informacijskih sistemov.

Velikost VOC v Evropi je tesno povezana s številom IP-naslovov, ki jih organizacija upravlja. Večje število IP-naslovov običajno pomeni potrebo po večjih in bolj strukturiranih VOC, naprednejših orodjih in pristopih ter uporabi segmentacije omrežij.

7 PRIMERJAVA VARNOSTNO-OPERATIVNIH CENTROV MED SLOVENIJO IN EVROPO

Varnostno-operativni centri so postali ključni obrambni mehanizmi v digitalnem okolju, saj predstavljajo operativno srce za zaznavanje, preprečevanje in obvladovanje kibernetskih incidentov. Medtem ko je vloga VOC splošno priznana tako v Sloveniji kot v drugih evropskih državah, se njihova zrelost, organizacija, tehnična opremljenost in regulatorna umeščenost med državami bistveno razlikujejo.

7.1 Institucionalni in pravni okvir

Učinkovitost varnostno-operativnih centrov je tesno povezana z zakonodajnim in institucionalnim okoljem, v katerem delujejo. V sodobni kibernetski arhitekturi ni dovolj, da VOC zgolj tehnološko spremljajo in analizirajo varnostne dogodke – njihovo delovanje mora biti usklajeno z nacionalnimi strategijami, regulativami in mednarodnim sodelovanjem. V tem kontekstu primerjava slovenskega in evropskega pravnega in institucionalnega okvira razkriva razlike, ki vplivajo na zrelost in učinkovitost VOC v praksi.

Nacionalni okvir v Sloveniji

Republika Slovenija je v letu 2025 sprejela Zakon o informacijski varnosti oz. krajše ZInfV-1, ki predstavlja temeljni zakonodajni dokument za vzpostavitev nacionalnega sistema informacijske in kibernetske varnosti. Zakon v pravni red prenaša določbe po direktivi NIS 2 in s tem Slovenijo formalno umešča v skupen evropski prostor kibernetske odpornosti.

ZInfV-1 opredeljuje ključne institucionalne nosilce:

- ***pristojni nacionalni organ*** (v praksi vloga pripada Uradu Vlade RS za informacijsko varnost), ki skrbi za usklajevanje ukrepov na državni ravni,
- ***skupine CSIRT***, ki opravljajo operativno odzivanje na incidente in svetovanje,
- ***enotna kontaktna točka***, ki predstavlja vmesnik med nacionalnimi subjekti in evropskimi varnostnimi strukturami,
- sistem zavezancev, ki so dolžni izvajati ukrepe za kibernetsko varnost ter poročati o incidentih in sodelovati s pristojnimi organi (Urad Vlade Republike Slovenije za informacijsko varnost, 2025).

Poleg tega zakon predvideva vzpostavitev strategije kibernetske varnosti, sistem nadzora in inšpekcijskih pregledov, obveznosti poročanja ter celo certifikacijo kibernetske varnosti za določene produkte in storitve. S tem se slovenska zakonodaja približuje zahodnim evropskim standardom, čeprav obstajajo izzivi predvsem na izvedbeni ravni.

Evropski okvir in institucionalni razvoj

Na ravni Evropske unije se področje kibernetske varnosti dinamično razvija od leta 2016, ko je bila sprejeta prva direktiva NIS, ki je danes nadomeščena z aktualno direktivo NIS 2. Ta je pomembno razširila obseg zavezancev, natančneje določila varnostne ukrepe in mehanizme nadzora ter postavila temelje za bolj sistematično usklajevanje držav članic (Direktiva 2022/2555, 2022).

Evropski pravni okvir temelji na naslednjih temeljnih institucionalnih strukturah:

- ENISA, ki deluje kot osrednji koordinator, svetovalec in izvajalec izobraževalnih ter raziskovalnih dejavnosti,
- CERT-EU, ki varuje institucije EU in deluje kot stičišče operativne podpore,
- EU-CyCLONe, ki omogoča koordinirano obvladovanje kibernetskih kriz velikih razsežnosti,
- CSIRT Network, ki združuje nacionalne odzivne skupine ter omogoča tehnično in operativno sodelovanje.

Države članice, kot so Nemčija, Francija, Nizozemska in Švedska, so VOC integrirale v svojo nacionalno varnostno strategijo že pred formalizacijo direktive NIS 2. Na primer, Nemčija znotraj zveznega urada za informacijsko varnost BSI upravlja lasten VOC in izvaja nadzor nad kritično infrastrukturo (Carrapico & Barrinha, 2018). Podobno francoski ANSSI (Agence nationale de la sécurité des systémes d'information) vodi lastne obrambne VOC-enote in zagotavlja nacionalno krizno koordinacijo.

Primerjalna analiza

Čeprav Slovenija z ZInfV-1 formalno vzpostavlja ustrezen pravni okvir, se dejanska institucionalna zrelost VOC še razvija. To se kaže v pomanjkanju specializiranih centrov, šibki integraciji z evropskimi strukturami in omejenem kadrovskem bazenu. Po drugi strani pa naprednejše države članice EU VOC že desetletje razvijajo kot strateške varnostne institucije,

ki sodelujejo na mednarodni ravni, upravljajo z obsežnimi podatkovnimi bazami o grožnjah in izvajajo celostne krizne scenarije.

Povezanost med nacionalnimi skupinami CSIRT in evropskimi strukturami v državah, kot so Estonija, Nizozemska in Danska, je bistveno bolj razvita kot v Sloveniji. Te države imajo operativne protokole za izmenjavo podatkov, interoperabilne sisteme in formalizirano sodelovanje v kibernetskih vajah EU.

7.2 Operativna struktura in zmogljivosti

Učinkovitost varnostno-operativnih centrov je v veliki meri odvisna od njihove notranje organiziranosti, jasno razdeljenih nalog, kadrovskih zmogljivosti in tehnološke podpore. Razlike med slovenskimi in evropskimi VOC so opazne tako v globini hierarhične razdelitve kot tudi v spektru specializiranih funkcij, ki jih centri opravljajo. Medtem ko v Sloveniji VOC praviloma še sledijo osnovni funkcionalni strukturi, so evropski primeri že integrirani v širše obrambne strategije organizacij in držav ter izkazujejo višjo stopnjo operativne zrelosti.

7.2.1 Struktura slovenskih VOC

V Sloveniji VOC pogosto delujejo kot podsklop notranjih IT-oddelkov v javnih ustanovah ali kot sestavni del varnostnih oddelkov v večjih podjetjih – zlasti v sektorjih, kot so bančništvo, energetika, telekomunikacija, gostovanje in upravljanje infrastrukture. Organizacijska struktura VOC je običajno razdeljena v dve osnovni operativni ravni:

- Nivo 1 (prva linija obrambe): primarna funkcija te ravni je spremljanje kibernetskih dogodkov, analiza opozoril iz sistemov SIEM, filtriranje *false positive* dogodkov in inicialna klasifikacija incidentov. Analitiki na tej stopnji pogosto opravljajo rutinske naloge brez širšega kontekstualnega razumevanja celotnega incidenta.
- Nivo 2 (druga linija obrambe): tu analitiki izvajajo poglobljeno tehnično analizo incidentov, preverjajo kompleksne alarme, izvajajo korelacijo podatkov in pripravljajo priporočila za nadaljnje ukrepanje. V tej fazi so analitiki pogosto tudi odgovorni za komunikacijo z uporabniki in interno eskalacijo incidentov.

Funkcija nivoja 3 je v Sloveniji redkeje prisotna znotraj internih VOC. Gre za raven, ki zajema napredno forenziko, analizo zlonamerne programske opreme, *threat hunting* in razvoj

obrambnih strategij. V mnogih primerih organizacije te storitve najamejo zunanje ponudnike – prek pogodbenih partnerjev, nacionalnega centra CSIRT ali zunanjih ponudnikov upravljanih varnostnih storitev MSSP.

7.2.2 Operativna razvejanost evropskih VOC

V naprednejših evropskih državah, kot so Estonija, Nemčija, Nizozemska in Finska, VOC predstavljajo osrednje vozlišče organizirane digitalne obrambe. Njihova operativna struktura presega tradicionalne tri stopnje analize in vključuje dodatne specializirane funkcije, kot so:

- ***Red teaming enote***: te specializirane ekipe izvajajo simulirane napade na lastno organizacijo z namenom testiranja njene odpornosti. Gre za etične hekerje, ki uporabljajo realistične metode napadalcev za preverjanje učinkovitosti obrambe, detekcije in odziva. Takšne enote pogosto sodelujejo z modro ekipo oz. *purple teaming* enotami (Cichnoski, Millar, Grance, & Scarfone, 2012).
- ***Napredna analiza zlonamerne programske opreme***: evropski VOC imajo pogosto lastne laboratorije za dinamično in statično analizo zlonamerne kode. S tem identificirajo zlonamerne vzorce, razvijajo signature in pripravljajo IOC (Indicators of Compromise), ki jih delijo z drugimi centri preko skupnih platform, kot sta MISP in OpenCTI (Cybersecurity, 2024).
- ***Avtomatizirano odzivanje***: z uvedbo sistemov SOAR evropski VOC znižujejo čas zaznavanja in odziva. SOAR omogoča avtomatsko izvajanje ukrepov, kot so izolacija naprave, ponastavitev poverilnic, opozorilo administratorju ali blokada IP-naslova v požarnem zidu. Poleg tega sistem omogoča ustvarjanje standardiziranih incidentnih *playbookov*, kar v enoti pripomore k sledljivi obravnavi incidentov (Kathryn Knerler, 2024).
- ***Threat intelligence celice***: napredni VOC vzdržujejo notranje ali hibridne *threat intelligence* oddelke, ki aktivno zbirajo, obdelujejo in distribuirajo informacije o grožnjah. Ti oddelki so pogosto povezani z zunanjimi repozitoriji podatkov in sodelujejo v pobudah za deljenje podatkov (Carrapico & Barrinha, European Union cyber security as an emerging research and policy field, 2018).

7.2.3 Povezovanje z nacionalnimi varnostnimi sistemi

Evropski VOC so operativno povezani z nacionalnimi centri CSIRT in agencijami za kibernetsko varnost ter sodelujejo v sistemih za krizno upravljanje. Delujejo tudi v okviru EU-CyCLONe, kjer se izvajajo scenariji odziva na incidente na ravni EU. Poleg tega VOC sodelujejo v vajah, kot je Cyber Europe, ki simulira množične kibernetske napade na kritično infrastrukturo in preizkuša odzivne zmogljivosti držav (ENISA, 2024 Report on the State of the Cybersecurity in the Union, 2024).

7.3 Tehnološka zrelost in avtomatizacija

Tehnološka zrelost in stopnja avtomatizacije varnostno-operativnih centrov predstavljata enega ključnih dejavnikov pri oceni njihove učinkovitosti, odzivnosti in dolgoročne kibernetske odpornosti. Medtem ko se številni evropski VOC naglo razvijajo v smeri popolnoma integriranih, avtomatiziranih in proaktivnih centrov, slovenski VOC še vedno v večji meri delujejo v okolju z omejenimi resursi, fragmentirano infrastrukturo in nizko stopnjo avtomatizacije.

7.3.1 Tehnološka raven slovenskih VOC

V Sloveniji VOC v veliki meri temeljijo na komercialnih platformah SIEM, kot sta IBM Qradar in Splunk, ki omogočata zbiranje, korelacijo in osnovno analizo dnevniških zapisov iz različnih virov. Čeprav ta orodja zagotavljajo osnovno operativno podporo, se njihova napredna funkcionalnost pogosto ne upravlja v celoti – predvsem zaradi pomanjkanja usposobljenega kadra, omejenih finančnih sredstev in nezadostne integracije z zunanjimi viri kibernetskih dogodkov.

Večina slovenskih VOC nima avtomatiziranega odziva na incidente. Ukrepi, kot so izolacija naprav, blokada IP-naslovov ali obveščanje prizadetih služb, se izvajajo ročno, kar povečuje odzivni čas in možnost napak. Tudi *threat intelligence* je pogosto omejen na ročno iskanje informacij po javno dostopnih virih, brez avtomatizirane integracije s platformami, kot so MISP, OpenCTI ali ThreatFox. Poleg tega je uporaba naprednih tehnik, kot so strojno učenje, anomalijska detekcija ali vedenjska analitika uporabnikov oz. krajše UEBA, v slovenskih VOC redka ali eksperimentalna. Organizacije so tako bolj reaktivne kot proaktivne, kar zmanjšuje možnost zgodnjega odkrivanja sofisticiranih groženj (SI-CERT, 2024).

7.3.2 Napredna avtomatizacija v evropskih VOC

Nasprotno pa so številni evropski VOC že na poti popolne digitalne transformacije. Ti centri uporabljajo kombinacijo naprednih varnostnih orodij in avtomatizacije, kar jim omogoča večjo učinkovitost, krajše odzivne čase in boljšo pokritost varnostnih incidentov.

Najpomembnejša orodja in tehnologije vključujejo:

- ***SOAR***: ti sistemi omogočajo avtomatizacijo odziva na incidente, izvajanja *playbookov*, orkestracijo med varnostnimi orodji in avtomatsko eskalacijo incidentov. Rešitve SOAR, kot so Cortex XSOAR, IBM Resilient in Splunk SOAR, so postale ključni sestavni del evropskih VOC.
- ***XDR***: sistemi XDR povezujejo podatke iz različnih varnostnih komponent (*endpointi*, omrežja, strežniki, aplikacije) v eno integrirano rešitev, ki omogoča boljše zaznavanje in odziv na kompleksne napade.
- ***UEBA***: sistemi UEBA analizirajo vedenjske vzorce uporabnikov in entitet v omrežju ter s pomočjo analitike in strojnega učenja zaznavajo nenavadno odstopanje, ki lahko kažejo na kompromitacijo znotraj sistema.
- ***AI/ML***: v mnogih evropskih VOC se uporablja umetna inteligenca za zaznavanje *zero-day* groženj, detekcijo zlorabe pravic in samodejno prilagajanje varnostnih politik. Primer take rešitve je Darktrace, ki temelji na avtonomni obrambi.

Poleg tehnološke naprednosti evropski VOC vzpostavljajo tudi strukturirane procese za krizno upravljanje – vključujejo incidente nadzorne plošče oz. angl. *dashboards* za odločevalce, redno izvajajo nacionalne krizne vaje, kot je ENISA Cyber Europe, in imajo formalizirane komunikacijske protokole za sodelovanje z državami in evropskimi organi (ENISA, 2024 Report on the State of the Cybersecurity in the Union, 2024).

7.4 Kadrovska struktura in usposobljenost

Usposobljenost kadrov in razvitost kadrovskih struktur varnostno-operativnih centrov igrata osrednjo vlogo pri zagotavljanju kibernetske varnosti. Kadri niso zgolj operativci – so analitiki, strateški svetovalci, raziskovalci groženj in krizni odločevalci. Razlike med kadrovskim stanjem v slovenskih in evropskih VOC so izrazite in vplivajo na odzivni čas, natančnost analiz in dolgoročno odpornost organizacij na kibernetske grožnje.

7.4.1 Kadrovski izzivi slovenskih VOC

Slovenski VOC, zlasti tisti, ki delujejo znotraj manjših organizacij ali državnih ustanov, delujejo z omejenimi kadrovskimi viri. Povprečni VOC obsega od 3 do 10 varnostnih analitikov, pri čemer en posameznik pogosto pokriva več funkcij hkrati – od osnovne analize dogodkov nivoja 1, poglobljene tehnične analize nivoja 2 in odziva na incidente do priprave poročil za vodstvo (SI-CERT, 2023).

Specializacija znotraj ekip je nizka, kar pomeni, da analitiki niso osredotočeni zgolj na določena področja (npr. digitalna forenzika ali *threat hunting*), temveč pogosto opravljajo vse naloge od začetka do konca incidenta. Takšen pristop lahko vodi v izgorelost, manjšo natančnost in počasnejše odzivanje – še posebej v obdobjih povišane ogroženosti.

Usposabljanja in certificiranja so v Sloveniji pogosto prepuščena notranjim mentorjem ali organizirana občasno in priložnostno, predvsem zaradi omejenih finančnih sredstev. Dostop do naprednih mednarodnih usposabljanj (npr. SANS Institut, Offensive Security) je omejen, prav tako tudi udeležba na evropskih varnostnih vajah ali programih izmenjave (ENISA, 2024 Report on the State of the Cybersecurity in the Union, 2024).

7.4.2 Napredne kadrovske strukture v evropskih VOC

VOC v razvitejših evropskih državah (npr. Nemčija, Nizozemska, Finska, Francija) imajo bolj modularno kadrovsko strukturo, kjer je vsak član ekipe specializiran za določeno funkcijo. Tipični kadrovski profili so:

- ***SOC Analyst (nivoja 1 in 2)***: osnovna in poglobljena analiza dogodkov;
- ***Incident Responder***: koordinacija in tehnični odziv na incidente;
- ***Threat Hunter***: proaktivno iskanje anomalij in skritih groženj;
- ***Digital Forensic Examiner***: analiza digitalnih dokazov, *reverse engineering* zlonamerne programske programske opreme;
- ***SOC Engineer***: tehnična podpora in konfiguracija varnostnih sistemov (npr. SIEM, SOAR);
- ***Threat Intelligence Analyst***: zbiranje in analiziranje podatkov o grožnjah iz odprtih in zaprtih virov (De Zan & Di Franco, 2019).

Poleg kadrovske raznolikosti imajo ti VOC dostop do strukturiranih nacionalnih in evropskih programov usposabljanja:

- ***CyberNet* –** evropski projekt, ki povezuje nacionalne skupine CSIRT in VOC ter omogoča prenos znanja, izmenjavo dobrih praks in organizacijo skupnih izobraževanj.
- ***EU Cybersecurity Skills Academy* –** pobuda Evropske komisije, katere cilj je povečati dostopnost in kakovost kibernetskih izobraževanj ter spodbujati pridobivanje certifikatov (Cybersecurity Skills Academy).
- ***ENISA Cyber Exercises* –** redne vaje, kot je Cyber Europe, v katerih sodelujejo evropski VOC, s čimer krepijo operativne sposobnosti in krizno komunikacijo (ENISA, 2024 Report on the State of the Cybersecurity in the Union, 2024).

Zaposleni v evropskih VOC pogosto posedujejo mednarodno priznane certifikate, ki potrjujejo njihovo strokovno usposobljenost:

- ***CISSP (Certified Information Systems Security Progessional)* –** strateška raven;
- ***GCIH (GIAC Cerified Forensic Analyst)* –** digitalna forenzika;
- ***OSCP (Offensive Security Ceritified Professional)* –** penetracijsko testiranje.

Takšni certifikati niso le potrdilo znanja, temveč predstavljajo vstopnico v kompleksnejše, avtomatizirane in integrirane strukture VOC.

7.4.3 Vplivi usposobljenosti na učinkovitost VOC

Pomanjkanje specializiranega kadra v Sloveniji pomeni, da so VOC manj proaktivni, pogosteje reaktivni in manj učinkoviti pri dolgoročnem obvladovanju tveganj. Poleg tega so odvisni od posameznikov, kar predstavlja tveganje ob menjavi osebja ali izgubi znanja.

Nasprotno pa evropski VOC gradijo odporne, standardizirane in nadomestljive strukture z visoko usposobljenim osebjem, ki omogoča večjo varnostno agilnost, hitrejše okrevanje po incidentih in zanesljivejše dolgoročno varovanje informacijskih sredstev.

7.5 Delovni obseg in pokritost

Slovenija: VOC v slovenskih organizacijah pogosto pokrivajo manjše število IP-naslovov in storitev, pri čemer je segmentacija omrežij pogosto osnovna. IP-segmentacija je uporabljena

funkcionalno (po oddelkih), redkeje pa vključuje napredno geolokacijsko ali tveganjsko razdelitev.

Evropa: VOC pokrivajo tisoče IP-naslovov in uporabljajo napredno segmentacijo omrežij – po tveganju, vrsti storitev, uporabnikih ali geografiji. To omogoča boljše zaznavanje anomalij in krajši odzivni čas (Kathryn Knerler, 2024).

7.6 Sodelovanje in integracija

Slovenski VOC šele v zadnjih letih povečujejo sodelovanje z nacionalnimi centri CSIRT, kot je SI-CERT, in šele vzpostavljajo sodelovanje s tujimi subjekti. Poročanje incidentov je pogosto reaktivno in formalno, brez aktivne obojestranske izmenjave podatkov.

Evropski VOC so pogosto že vključeni v mreže EU-CSIRT, sodelujejo v vaji Cyber Europe, delujejo v okviru EU-CyCLONe in imajo stalne kanale z avtomatizirano izmenjavo podatkov o grožnjah z organi EU in sosednjimi državami (ENISA, 2024 Report on the State of the Cybersecurity in the Union, 2024).

8 PRIPRAVA VZORCA DELOVNEGA PROTOKOLA

Vzpostavitev celovitega in učinkovitega delovnega protokola za varnostno-operativni center predstavlja ključen korak k standardizaciji postopkov, povečanju kibernetske odpornosti in skladnosti z zakonodajnimi okviri, kot so Zakon o informacijski varnosti, direktiva NIS 2 ter ISO/IEC 27001. Namen tega poglavja je predstaviti strukturiran vzorec delovnega protokola, ki pokriva vse ključne funkcionalne in varnostne zahteve sodobnega VOC.

8.1 Namen in cilji protokola

Osnovni namen delovnega protokola za varnostno-operativni center je oblikovanje enotnih, sledljivih in zakonsko skladnih postopkov za zaznavanje, analizo, odzivanje in poročanje o kibernetskih varnostnih dogodkih. Protokol deluje kot formaliziran dokument, ki podaja operativni okvir za vse ključne procese znotraj VOC, zmanjšuje možnost napak, omogoča konsistentnost pri odzivanju ter skrbi za usklajenost z notranjimi politikami in zunanjo zakonodajo.

Vsebinsko protokol definira:

- vloge in odgovornosti vseh udeležencev, kot so analitiki od nivoja 1 do nivoja 3, vodje izmen, inženirji, skrbniki sistemov ter odgovorne osebe za obveščanje poročanja;
- pravila dostopa do varnostnih orodij in sistemov, ki temeljijo na načelu najmanjših pravic ter vključujejo večstopenjsko preverjane pristnosti (npr. MFA, ločeni *admin* računi);
- obveznosti glede komunikacije znotraj ekipe in navzven, vključno z obveščanjem pristojnih deležnikov;
- postopke dokumentiranja in arhiviranja incidentov, ki zagotavljajo sledljivost, revizijsko pregledanost ter izpolnjevanje zahtev standardov ISO/IEC 27001 in ISO/IEC 27035.

Dolgoročni cilji protokola vključujejo:

- vzpostavitev kulture varnosti in odgovornosti znotraj organizacije,
- standardizacijo postopkov v vseh izmenah in izogibanje neformalnim rešitvam,
- zagotavljanje podlage za notranje presoje, zunanje nadzore in stalno izboljševanje sistema upravljanja informacijske varnosti,

- izboljšanje učinkovitosti odziva na incidente in krajšanje časa zaznave ter časa odprave incidenta,
- olajšanje uvajanja novega osebja s pomočjo strukturiranih in ponovljivih postopkov.

Z vidika organizacije protokol VOC omogoča tudi zmanjševanje odvisnosti od posameznikov, saj celotno znanje in praksa postaneta del dokumentiranega sistemskega pristopa. Poleg tega služi kot podlaga za redne vaje, simulacije incidentov in razvoj kriznih scenarijev.

Z vključevanjem navodil, opozoril, predlog procesnih tokov in jasnih definicij v vloge vsakega člana ekipe protokol pripomore k temu, da VOC postane profesionalna, odzivna in zakonodajno skladna enota v sodobni kibernetski arhitekturi organizacije.

8.2 Zakonski in standardni okvir

Delovni protokol varnostno-operativnega centra mora biti zasnovan skladno z veljavno zakonodajo, mednarodnimi standardi in uveljavljenimi smernicami dobre prakse. Ta okvir zagotavlja pravno varnost, omogoča revizijsko sledljivost in predstavlja temelj za organizacijsko zrelost ter dolgoročno skladnost delovanja VOC.

8.2.1 Ključni zakonski akti

Zakon o informacijski varnosti je temeljni nacionalni pravni akt, ki opredeljuje pravila za zaščito informacijskih sistemov, vlogo nacionalnih skupin CSIRT in obveznosti zavezancev ter prenaša v slovenski pravni red zahteve evropske direktive NIS 2. Zakon predpisuje minimalne varnostne ukrepe, postopke poročanja o incidentih, postopke izvajanja ocene tveganj ter vzpostavlja nadzorne in inšpekcijske mehanizme.

Direktivna NIS 2 določa skupne ukrepe držav članic za dosego visoke skupne ravni kibernetske varnosti v EU. Med ključnimi zahtevami so:

- razširitev kroga zavezancev,
- obveznost obveščanja o incidentih v določenih rokih,
- imenovanje varnostno odgovornih oseb,
- upravljanje z dobavitelji in tveganji tretjih strani,
- obveznosti glede notranjih politik, postopkov in testiranj.

Uredba (EU) 2019/881 (Cybersecurity Act) ureja delovanje evropskega ogrodja za kibernetsko varnost, vključno z okrepljeno vlogo agencije ENISA in vzpostavitvijo shem certificiranja kibernetske varnosti na ravni EU. VOC morajo upoštevati certifikacijske zahteve za varnostne produkte in storitve, kjer je to relevantno.

8.2.2 Mednarodni standardni

Protokol je usklajen z naslednjimi standardi:

- ISO/IEC 27001:2022 – standard za sisteme upravljanja informacijske varnosti (ISMS), ki opredeljuje zahteve za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje varnostnega sistema. VOC mora znotraj ISMS pokrivati tudi odzivanje na incidente in vodenje evidenc.
- ISO/IEC 27034 – standard, ki podrobneje ureja proces obvladovanja varnostnih incidentov, od pripravljenosti do zaznavanja, analize, odziva in učenja dogodkov.

8.2.3 Operativne smernice in modeli

Delovni protokol se naslanja na uveljavljene operativne modele in referenčne okvirje, kot sta:

- MITRE ATT&CK Framework – taksonomija taktik, tehnik in postopkov napadalcev (TTP), ki se uporablja za izboljšano zaznavanje in razumevanje varnostnih groženj ter za oblikovanje detekcijskih pravil in *playbookov* v sistemih SIEM/SOAR.
- 11 Strategies of a World-Class SOC – publikacija MITRE, ki podaja konkretna priporočila glede strukturiranja ekip SOC, avtomatizacije, odzivanja, sodelovanja z vodstvom in merjenja učinkovitosti delovanja centra.

8.2.4 Priporočila strokovnih teles

- ENISA (European Union Agency for Cybersecurity) redno izdaja poročila, tehnične smernice in priporočila, vezana na operativno zmogljivost VOC, odzivanje na incidente, sodelovanje s centri CSIRT in ocenjevanje groženj.

- Nacionalni centri CSIRT (npr. SI-CERT v Sloveniji) nudijo priporočila za obravnavo aktualnih groženj, organizirajo krizne vaje in zagotavljajo operativno podporo v primeru večjih incidentov.

8.3 Vsebina protokola

Delovni protokol varnostno-operativnega centra predstavlja osrednji dokument za vzpostavitev standardiziranih, ponovljivih in revizijsko sledljivih varnostnih praks. Njegova vsebina pokriva širok spekter funkcionalnih področij, ki so potrebna za neprekinjeno delovanje VOC, učinkovito odzivanje na kibernetske incidente in usklajeno sodelovanje med deležniki znotraj in zunaj organizacije.

8.3.1 Organizacija delovnega dne in izmen

VOC mora delovati neprekinjeno vse dni v letu, običajno v triizmenskem režimu. Protokol določa:

- časovne okvire in odgovornosti posameznih izmen,
- postopke predaje izmene, vključno z evidenco odprtih incidentov, operativnimi opozorili in statusi sistemov,
- nadomestne režime v primeru kadrovskih odsotnosti ali povečanega obsega dela,
- aktivacijo kriznih režimov, ko incidenti presegajo zmogljivosti rednega osebja (npr. aktivacija ekipe *incident response team* ali eskalacija vodstvu organizacije).

Takšna organiziranost prispeva k nemotenemu prenosu informacij med izmenami in zmanjšuje tveganje operativnih vrzeli.

8.3.2 Operativni postopki

Jedro delovnega protokola predstavljajo operativni postopki, med katere spadajo:

- klasifikacija dogodkov glede na kritičnost, vpliv in verodostojnost,
- *triage*, kjer analitiki nivoja 1 preverijo pomembnost dogodka, filtrirajo *false-positive* dogodke in eskalirajo pomembne incidente,

- uporaba ključnih orodij, kot so:
  - SIEM (npr. Splunk, Qradar …) za korelacijo dogodkov,
  - SOAR za avtomatizacijo odziva in orkestracijo ukrepov,
  - EDR/XDR za spremljanje in odzivanje na dogodke na končnih točkah (*endpoints*),
- analiza in *containment* – poglobljena tehnična preiskava incidentov ter omejevanje širjenja,
- remediacija in obnovitev – odprava posledic incidenta ter povrnitev prizadetih sistemov.

Postopki so definirani v obliki t. i. *playbookov*, ki zagotavljajo konsistentno in hitro delovanje ekipe.

8.3.3 Komunikacija

Učinkovita in varna komunikacija je ključna komponenta vsakega protokola VOC. Protokol določa:

- notranje komunikacijske poti med ekipo VOC, IT-podporo, pravno službo, vodstvom in PR-oddelkom,
- zunanje komunikacije z nacionalnim CSIRT, regulatorji, partnerji in uporabniki,
- kanale komunikacije, ki vključujejo varne komunikacijske platforme, e-pošto z elektronskim podpisom, šifrirane glasovne klice itd.,
- postopke obveščanja, kjer se natančno določi, kdo, kdaj in kako mora biti obveščen glede na tip in obseg incidenta.

Pri kritičnih incidentih se sproži tako imenovan *incident communication plan*, ki določa tok informacij v realnem času.

Ovrednotenje H1: intervjuji s strokovnjaki potrjujejo, da so se kljub obstoječim protokolom pojavile vrzeli (nejasna poročevalska veriga, neaktualiziran živ protokol), kar kaže, da dokumentacija v praksi ni vedno dovolj jasna.

8.3.4 Preventivni ukrepi

VOC ni le reaktivna enota, temveč mora izvajati tudi proaktivne varnostne ukrepe, kot so:

- *purple teaming* simulacije, kjer *red teaming* enote testirajo zmogljivosti detekcije in odzivanje ob sodelovanju z *blue teaming* osebjem,
- upravljanje ranljivosti, ki vključuje redno izvajanje skenov ranljivosti, ocenjevanja kritičnosti in prioritizacijo popravkov,
- testiranje konfiguracij in skladnosti varnostnih politik,
- varnostna obvestila in kampanje ozaveščanja zaposlenih, kar pripomore k zmanjšanju napak človeškega faktorja.

Ovrednotenje H4: dokumentiran delovni protokol, urejena baza znanja in *checkliste* dokazano pospešijo uvajanje novih članov SOC ter pomagajo vzdrževati kibernetsko higieno (npr. MFA, posodobitve, zaklepanje postaj); *playbooki* so posebej pomembni za hitro uvedbo novih kadrov do samostojnosti ter vodenje evidenc in dokumentacije.

Sistematično vodenje evidenc zagotavlja sledljivost, skladnost z zakonodajo in učinkovit nadzor. Protokol določa:

- *ticketing* sistem,
- revizijske sledi,
- evidence obravnavanih dogodkov in časovnih odzivov,
- dokumente *lessons-learned*, ki povzemajo ugotovitve po zaključenih incidentih in predlagajo izboljšave.

Vsa dokumentacija mora biti hranjena skladno z internimi pravilniki in določili GDPR.

8.3.5 Fizična logična varnost

Protokol določa ukrepe za zagotavljanje fizične varnosti prostorov VOC in logične zaščite digitalnega okolja:

- večnivojski fizični dostop, vključno z elektronskimi karticami, biometričnimi prijavami in spremljanjem vstopov,
- segmentacija omrežij z uporabo požarnih zidov, VLAN-ov in mikrosegmentacije,
- večstopenjska avtentikacija (MFA), uporaba enkratnih gesel (OTP) in ločenih računov za privilegirane dostope (PAM),

- ločevanje razvojnega, testnega in produkcijskega okolja,
- šifriranje komunikacij in varnostnih kopij z uporabo standardov AES-256 ali višje.

Vsebina delovnega protokola VOC mora biti dovolj celovita, da pokriva tako vsakodnevno delovanje centra kot tudi odzivanje v izrednih situacijah. S tem ko protokol usklajuje operativne postopke, komunikacijske poti, preventivne prakse in zahteve po dokumentiranju, zagotavlja podlago za učinkovit, pregleden in zakonsko skladen sistem obvladovanja kibernetskih incidentov.

8.4 Operativni cikli in standardizacija

Učinkovitost varnostno-operativnega centra je v veliki meri odvisna od konsistentnega, standardiziranega izvajanja ključnih nalog, ne glede na čas dneva ali posamezno izmeno. Glede na naravo kibernetskih groženj, ki so lahko nepredvidljive in časovno nenadne, mora VOC delovati neprekinjeno (24/7) v strogo organiziranih triizmenskih ciklih z jasno določenimi nalogami, roki in postopki.

Ovrednotenje H2: strokovni sogovorniki navajajo, da standardizirani protokoli omogočajo hitrejši, usklajen in ponovljiv odziv v kriznih dogodkih. Čeprav so dogodki raznoliki, standardi dokazano olajšajo reševanje in izboljšujejo pripravljenost.

8.4.1 Triizmenski režim delovanja

VOC običajno sledi rotacijskemu urniku z naslednjimi značilnostmi:

- jutranja, popoldanska in nočna izmena (vsakih 8 ur),
- določeni odgovorni za vodje izmene,
- predpisana rotacija vlog znotraj izmene (npr. analitik A za *triage*, analitik B za *containment*),
- nadomestne ekipe in krizni režimi (npr. ob večjem incidentu se aktivira *incident response* ekipa ne glede na delovni čas).

Vsaka izmena mora prevzeti in oddati delo s formalno predajo izmene, da se zagotovi kontinuiteta operacij in sledljivost obravnavanih dogodkov.

8.4.2 Ključni operativni postopki v ciklu

V vsakem operativnem ciklu VOC izvaja niz ponavljajočih se nalog, ki so jasno dokumentirane in nadzorovane:

- Redni *health-check* sistemov – zajema preverjanje razpoložljivosti ključnih orodij, kot so SIEM, SOAR, EDR, in zbiralnikov logov, preverjanje povezav z nadzorovanimi sistemi, stanje varnostnih posodobitev in morebitne alarme.
- Pregled dnevnih KPI-jev – analiza uspešnosti iz prejšnje izmene, vključno s:

– številom obravnavanih dogodkov,

– odzivnim časom (MTTD, MTTR),

– deležem *false positive* dogodkov,

– neobravnavanimi ali eskaliranimi incidenti.

- Evidentiranje in obravnava dogodkov – vključuje dokumentiranje vseh zaznanih varnostnih dogodkov, klasifikacijo po pomembnosti, sprožitev ustreznih *playbookov* in ažurno beleženje v *ticketing* sistem.
- Formalna predaja izmene z uporabo strukturiranega obrazca, npr. Change-of-Shift Report, ki vključuje:

– odprte incidente in njihov status,

– sisteme, ki so v nadzoru ali izolaciji,

– pomembna opozorila in zaznane nepravilnosti,

– navodila in priporočila naslednji izmeni.

Ti postopki so ključni za operativno doslednost, zmanjševanje človeških napak in zagotavljanje neprekinjenega nadzora nad varnostjo informacijskega okolja.

8.4.3 Standardizacija z obrazci in postopki

Standardizacija poteka s pomočjo:

- obrazcev, kot so:

– Daily Check Log (za *health-checke*),

– KPI Summary Sheet (za metrike uspešnosti),
– Incident Timeline Sheet (za pregled eskaliranih incidentov),
– Lessons Learned Template (po večjih incidentih),

- *checklist* postopkov, ki zagotavljajo, da vsaka izmena izvede ključne naloge v skladu s pričakovanji,
- usposabljanja novega osebja, kjer se standardizirani postopki uporabljajo kot orodje za hitro uvedbo in zmanjšanje napak.

Ovrednotenje H3: sogovorniki pravijo, da se zaposleni pogosto opirajo na osebne izkušnje, medtem ko redno posodabljanje baz znanja, *checkliste* in *flowcharti* zmanjšujejo odvisnost od posameznikov in pospešijo reševanje primerov.

8.4.4 Vloga avtomatizacije

V zrelejših okoljih VOC številne postopke že avtomatizirajo z uporabo sistemov SOAR, ki avtomatsko:

- preverjajo stanje sistemov,
- poročajo o dostopanjih v KPI-jih,
- sprožijo opozorila ob izjemah,
- generirajo obrazce za poročanje ob koncu izmene.

S tem se sprosti čas analitikov za kompleksnejše naloge, zmanjša se obremenjenost in poveča natančnost pri poročanju.

Jasen, dokumentiran in ponovljiv operativni cikel je bistven za učinkovito delovanje VOC. Standardizacija postopkov skozi izmensko delo, avtomatizirane naloge in strukturirano poročanje omogoča stabilno delovanje tudi v pogojih visoke ogroženosti. Formalna predaja izmene in sledenje KPI-jem tvorita hrbtenico nadzora nad kakovostjo operacij in prispevata k stalnemu izboljševanju delovanja centra.

8.5 Varnostna tveganja in kontrolni ukrepi

VOC se v vsakodnevnem delovanju sooča s številnimi kibernetskimi tveganji, ki izvirajo iz zunanjih groženj, internih ranljivosti in človeškega faktorja, zato mora delovni protokol vsebovati strukturirano analizo tveganj ter ustrezne kontrolne ukrepe, ki zmanjšujejo verjetnost uresničitve grožnje in blažijo njen vpliv na informacijsko okolje.

8.5.1 Analiza tveganj

VOC mora redno izvajati sistematično identifikacijo in ocenjevanje tveganj, ki vključuje naslednje kategorije:

- Socialni inženiring – napadi z uporabo psihološke manipulacije (*phising*, *vishing*, *pretexting*), ki ciljajo na zaposlene z dostopom do varnostnih sistemov.
- Zlonamerna programska oprema – vnos preko e-pošte, prenosljivih medijev ali ranljivosti sistema.
- Notranje grožnje – namerni ali nenamerni varnostni incidenti, ki jih povzročijo zaposleni.
- Napake v procesih – neupoštevanje operativnih protokolov, pomanjkanje dokumentacije, nepregledne eskalacije incidentov.
- Tehnične ranljivosti – zastarela programska oprema, nepravilno konfigurirani sistemi, nešifrirane komunikacije.

Za oceno tveganj se priporoča uporaba matrike verjetnosti in vpliva, kjer se tveganja ovrednotijo na podlagi kvantitativnih ali kvalitativnih kriterijev.

8.5.2 Ključni kontrolni ukrepi

Na podlagi analize tveganj se v delovni protokol vključijo naslednji ključni kontroli ukrepi:

- MFA (Multi-Factor Authentication) – zagotavlja, da za dostop do kritičnih sistemov uporabniki uporabljajo več neodvisnih oblik preverjanja pristnosti (geslo, mobilna aplikacija, pametna kartica).

- PAM (Privileged Access Managment) – sistem upravljanja privilegiranih dostopov, ki omogoča časovno omejen dostop do občutljivih sistemov, nadzor uporabe administratorskih računov in revizijsko sledljivost.
- Simulirani napadi (*red teaming*) – redno izvajanje simulacij realističnih napadov, ki preizkusijo odzivne zmogljivosti VOC in razkrijejo varnostne vrzeli v postopkih, orodjih ali kadru.
- Kriptografsko podpisovanje dnevnikov – zagotavlja celovitost in avtentičnost varnostnih dnevnikov (npr. SIEM logi), kar je ključno za revizije in forenzično analizo po incidentih.
- Segmentacija omrežja – delitev omrežnega okolja na logične cone (npr. po funkciji, lokaciji, kritičnosti) s ciljem omejevanja lateralnega gibanja in boljšega nadzora nad prometom.
- Pravilo najmanjših pravic – vsakemu uporabniku, procesu ali napravi se dodelijo zgolj tiste pravice, ki so nujno potrebne za izvajanje nalog, kar zmanjšuje potencialno škodo ob zlorabi ali napaki.

8.5.3 Matrika tveganj in kontrol

Sestavni del protokola je tudi matrika tveganj in pripadajočih kontrol, kjer so za vsako identificirano tveganje določeni:

- opisi grožnje in ranljivosti,
- ocena verjetnosti in vpliva,
- obstoječi in predlagani ukrepi,
- odgovorne osebe in roki za izvajanje,
- status ukrepa (v izvajanju, implementiran, preverjen).

8.5.4 Povezanost s standardi

Izvedba analize tveganj in opredelitev kontrolnih ukrepov je skladna z zahtevami:

- ISO/IEC 27001 – aneks (upravljanje dostopov, kriptografija, fizična varnost),
- ISO/IEC 27005 (upravljanje tveganj informacijske varnosti),

- ZInfV-1, ki predvideva izvajanje ustreznih varnostnih ukrepov glede na oceno tveganja,
- NIS 2, ki zavezancem nalaga vzpostavitev sistema za obvladovanje tveganj, vključno z obvladovanjem varnostnih verig dobaviteljev.

Delovni protokol VOC ni zgolj operativni priročnik, temveč tudi orodje za sistematično obvladovanje tveganj. Z vključevanjem ustreznih kontrolnih ukrepov na področju dostopov, nadzora, preverjanja in simulacijskih vaj VOC zmanjšuje svojo izpostavljenost grožnjam in povečuje odpornost informacijskega sistema. S tem postane ne le reaktivna, temveč tudi proaktivna obrambna enota v kibernetskem prostoru.

8.6 Skladnost in revizija

Skladnost z zakonodajo, regulatornimi zahtevami in notranjimi pravilniki je ključni element učinkovitega delovanja varnostno-operativnega centra. Protokol mora omogočati ne le tekoče operativno izvajanje nalog, temveč tudi sistematično spremljanje skladnosti ter redne notranje presoje in zunanje revizije, ki preverjajo učinkovitost, doslednost in zakonsko ustreznost delovanja centra.

8.6.1 Zakonodaja in standardna skladnost

VOC mora skladno delovati z naslednjimi ključnimi pravnimi in standardnimi okvirji:

- Zakon o informacijski varnosti – VOC mora kot enota v organizacijah, ki sodijo med zavezance po zakonu, izvajati redne ocene tveganj, voditi evidence o incidentih in zagotavljati postopke obveščanja organov CSIRT.
- Splošna uredba o varstvu podatkov – VOC mora zagotoviti varnost osebnih podatkov, spremljati dostop do informacijskih sistemov in beležiti dogodke, ki bi lahko ogrozili pravice posameznikov.
- ISO/IEC 27001:2022 – standard upravljanja informacijske varnosti, ki med drugim predpisuje zahteve za izvajanje notranjih presoj ISMS, analizo tveganj, revizijo varnostnih ukrepov in korektivne ukrepe.

8.6.2 Notranje presoje ISMS

VOC mora redno izvajati notranje presoje, bodisi v okviru oddelka za skladnost bodisi s pomočjo zunanjih presojevalcev. Ključna področja, ki jih protokol vključuje v sistem notranjega nadzora, so:

- Preverjanje izvedbe protokola – ali zaposleni delujejo skladno z definiranimi *playbooki*, ali obstajajo dostopanja in kako se ta dokumentirajo.
- Revizija dostopov – redna kontrola privilegiranih dostopov do sistemov (npr. SIEM, SOAR, EDR), preverjanje skladnosti z načelom najmanjših pravic in revizija sprememb nastavitev.
- Preverjanje izvedenih usposabljanj – protokol predvideva, da vsak zaposleni opravi začetno usposabljanje, letno obnovo znanja in sodeluje pri vajah. Te aktivnosti se dokumentirajo in preverjajo v revizijskih pregledih.
- Analiza kazalnikov učinkovitosti – VOC spremlja in analizira ključne KPI-je, kot so:

– MTTD (Mean Time to Detect) – povprečni čas od začetka incidenta do zaznave,

– MTTR (Mean Time to Respond) – povprečni čas do popolnega odziva ali rešitve,

– stopnja ponovitve incidentov, število *false positives*, odzivni čas izmene itd.

Te matrike omogočajo oceno uspešnosti delovanja VOC, identifikacijo ozkih grl in načrtovanje izboljšav.

8.6.3 Zunanje presoje in nadzori

Poleg notranjih pregledov je VOC pogosto predmet zunanjih revizij, ki jih lahko izvajajo:

- nadzorni organi (npr. informacijski pooblaščenec, AKOS),
- nacionalni CSIRT (npr. SI-CERT),
- zunanji revizorji v okviru certificiranja po ISO/IEC 27001 ali drugih standardih (npr. ISO 22301, ISO 20000).

Zunanji pregledi praviloma vključujejo preverjanje skladnosti s predpisi, zmožnost hitrega in učinkovitega odziva ter stopnjo zrelosti varnostnega upravljanja.

8.6.4 Nenehno izboljševanje

VOC mora v okviru delovnega protokola vključiti tudi mehanizme za stalno izboljševanje (PDCA – Plan, Do, Check, Act). Na podlagi revizijskih ugotovitev in analiz KPI-jev se izvajajo:

- korektivni in preventivni ukrepi (CAPA),
- posodabljanje protokola, orodij in varnostnih politik,
- razvoj novih *playbookov* ali optimizacija obstoječih,
- načrtovanje dodatnih usposabljanj ali kadrovskih okrepitev.

Redno preverjanje skladnosti z zakonodajo, standardi in notranjimi postopki je ključno za učinkovito delovanje in dolgoročno zanesljivost VOC. Sistematične presoje in metrika uspešnosti omogočajo ne le nadzor, ampak tudi strateško izboljševanje varnostnega upravljanja. VOC, ki aktivno izvaja notranje revizije in spremlja učinkovitost, dosega višjo stopnjo zrelosti in pripravljenosti na sodobne kibernetske grožnje.

9 OVREDNOTENJE HIPOTEZ IN ODGOVORI NA RAZISKOVALNA VPRAŠANJA

Namen naloge je bil opredeliti in standardizirati delovni protokol varnostno-operativnega centra ali krajše VOC, preveriti njegovo vlogo pri zaznavanju, obvladovanju in preprečevanju kibernetskih dogodkov ter ovrednotiti zrelost praks v Sloveniji v primerjavi z razvitejšimi evropskimi okolji. Uporabljena metodologija je združila analitični pregled operativnih zahtev, normativni/standardni okvir in kvalitativne vpoglede iz dveh polstrukturiranih intervjujev ob podpori priporočenih praks Mitre. V intervjujih so sodelovali vodja VOC, menedžer VOC, vodje informacijske varnosti (CISO) in etična hekerka. Sklep temelji na triangulaciji teh treh virov.

9.1 Ovrednotenje hipotez

9.1.1 Ovrednotenje H1

Vsi delovni protokoli v centrih VOC niso dovolj jasno dokumentirani.

Hipoteza je podprta. Izjave sogovornikov navajajo nejasnosti pri eskalaciji, poročanju in komunikacijskih poteh (npr. nedoločeni kanali in odgovorne osebe), pa tudi vrzeli v bazi znanja pri redkih ali kompleksnih scenarijih; to vodi v odločitve »po občutku« in neenotno izvedbo. ZInfV-1 zahteva sledljivo varnostno dokumentacijo in urejene protokole obveščanja CSIRT, zato pomanjkljiva dokumentiranost predstavlja tudi skladnostno tveganje.

9.1.2 Ovrednotenje H2

Standardizirani protokoli so ključni za učinkovito delovanje VOC v kriznih situacijah.

Hipoteza je podprta. Intervjuji potrjujejo, da SOP-ji/*playbooki* omogočajo hiter, usklajen in ponovljiv odziv ter zmanjšajo izgubo časa pri odločanju. Učinke je mogoče kvantificirati z metrikami (npr. odzivni čas). MITRE izrecno priporoča formalizirane postopke, predaje izmen in KPI-je (MTTD/MTTR) kot nosilce *world-class* zrelosti SOC.

9.1.3 Ovrednotenje H3

Ustrezno dokumentirani protokoli zmanjšujejo odvisnost od posameznih izkušenih zaposlenih.

Hipoteza je podprta. V praksi se odločitve pogosto naslanjajo na rutino izkušenejših. Kjer pa obstajajo sproti posodobljena baza znanja, *checkliste* in *flowcharti*, lahko manj izkušeni vodijo enotne postopke brez stalne pomoči.

9.1.4 Ovrednotenje H4 (BTEC 2025)

Uvajanje novih zaposlenih v VOC je hitrejše in učinkovitejše, če organizacija uporablja dokumentiran protokol dela in skrbi za kibernetsko higieno.

Hipoteza je podprta. Strokovnjaki pri intervjuju potrjujejo, da strukturiran *onboarding* (jasni postopki, sledenje izkušenim, urejena baza znanja) skrajša čas do samostojnosti in utrjuje higienske prakse (MFA/2FA, posodobitve, zaklepanje postaj, takojšnje poročanje o primeru varnostnih dogodkov). Dodatno je hipoteza skladna z dispozicijo BTEC.

9.2 Opredelitev raziskovalnih vprašanj

Kako je strukturirano delo analitikov VOC po različnih stopnjah (nivoji 1, 2, 3 in vodja VOC)?

Model vlog je v Sloveniji in Evropi načeloma homogen: nivo 1 izvaja neprekinjen nadzor, *triage* in validacijo. Nivo 2 vodi tehnično preiskavo, *containment* in koordinacijo z IT. Nivo 3 pokriva *threat hunting*, forenziko in razvoj detekcij. Vodja izmene/VOC skrbi za prioritetizacijo in neprekinjeno pokritost.

Kakšna je zrelost VOC v Sloveniji v primerjavi z razvitejšimi evropskimi državami?

Pri večjih/bistvenih subjektih je zrelost primerljiva (SOP, ISMS, KPI), vrzeli pa so najpogosteje v obsegu avtomatizacije SOAR, dosledni rabi metrik in stalni prisotnosti; v naprednejših okoljih je več proaktivnega *huntanja*, integriranih *intel* verig in ekosistemskih vaj.

Kako pomembna je prisotnost človeškega faktorja v okoljih VOC kljub avtomatizaciji?

Avtomatizacija razbremeni rutino, ne nadomesti pa kontekstualne presoje, komunikacije in odločanja pod časovnim pritiskom; kritična sta kultura »po postopkih« in stalno usposabljanje, kar terja tudi ZInfV-1.

Kako VOC zagotavljajo odziv na incidente v realnem času in kakšna je njihova učinkovitost?

Učinkovitost temelji na dobro nastavljenih tokovih SIEM/SOAR/EDR, vnaprej definiranih *playbookih*, SLA-jih in jasnih eskalacijah; MTTD/MTTR se znižata, ko so procesi standardizirani, vloge jasne, *health-checki* dosledni in učenje po incidentih sistematično.

Kako pomembna je vloga sistemov za odkrivanje, preprečevanje in analizo kibernetskih dogodkov pri vsakodnevnem delu analitika na VOC?

SIEM (korelacija/vidljivost), EDR/XDR (*endpoint* odziv), SOAR (orkestracija/avtomatizacija) ter skenerji ranljivosti in *sandboxi* predstavljajo jedro ponovljive, merljive operativnosti VOC.

V kolikšni meri se slovenske in evropske organizacije prilagajajo zahtevam direktive NIS 2?

Napredek je neenakomeren: največji je pri kritični infrastrukturi in večjih ponudnikih, izzivi pa vključujejo obvladovanje dobaviteljev, dokazljivost ukrepov, formalizirano poročanje in usposabljanja. ZInfV-1 postavlja obveznosti upravljanja tveganj, dokumentacije in poročanja.

Kako organizacije v Sloveniji upravljajo tveganja glede tretjih strani (dobaviteljskih verig) znotraj operacij VOC?

Uveljavlja se kombinacija pogodbenih zahtev, vprašalnikov, razvrščanja dobaviteljev po tveganju in spremljanja dogodkov; vrzeli so v stalnem monitoringu in v *shadow* IT-ju. VOC mora imeti posebne *playbooke* za incidente glede tretjih strani.

Kakšno vlogo ima sodelovanje VOC z nacionalnimi in evropskimi varnostnimi organi?

Ključna sta pravočasno obveščanje in izmenjava indikatorjev po TLP, podprta z vnaprej določenimi komunikacijskimi protokoli in kontaktnimi seznami; to zmanjšuje odzivni čas in skladnostna tveganja.

Kako se bo po pričakovanjih razvijala vloga VOC v naslednjih letih v Sloveniji in Evropi?

Pričakovati je več avtomatizacije SOAR, konvergence XDR, podporo AI pri *triage*, *cloud-native* nadzor, hibridne modele z MSSP/MDR ter več proaktivnega *huntanja* in sektornih vaj; regulatorni okvir bo pospeševal profesionalizacijo metrik in poročanja.

Kakšno vlogo ima delovni protokol pri zagotavljanju učinkovitega delovanja VOC pri zaznavanju, obvladovanju in preprečevanju incidentov?

Protokol je »operativna ustava« VOC: standardizira postopke, zmanjšuje napake med izmenami, pospešuje *onboarding*, omogoča sledljivost in revizijsko dokazljivost ter podpira skladnost po ZInfV-1.

Kako lahko strukturiran delovni protokol prispeva k izboljšanju sodelovanja med deležniki znotraj VOC in z zunanjimi partnerji?

Jasne vloge, komunikacijska matrika, kanali in predloge sporočil izboljšajo usklajenost IT-ja, pravne službe, vodstva, PR-ja in centra CSIRT, zmanjšajo podvajanja in nesporazume ter olajšajo integracijo partnerjev.

Kaj pomeni fleksibilnost za uspešnost izvajanja storitev VOC?

Uspešnost zahteva ravnotežje med dosledno standardizacijo in agilno prilagodljivostjo (*surge* kapacitete, modularna arhitektura, *risk-based* prioritetizacija); *playbooki* morajo biti »živi« in prilagodljivi.

10 SKLEP

Namen naloge je bil celostno osvetliti vlogo varnostno-operativnih centrov (VOC) pri odkrivanju, preprečevanju in analizi kibernetskih dogodkov v slovenskem in širšem evropskem prostoru. Osredotočili smo se na organizacijsko strukturo in delitev odgovornosti po ravneh (nivoji 1–3 in vodja VOC), pomen človeškega faktorja v okoljih visoke avtomatizacije, operativno učinkovitost odzivanja v realnem času, skladnost z regulativnimi zahtevami ter upravljanje tveganj dobaviteljskih verig in sodelovanje z zunanjimi deležniki. S pristopom, ki združuje pregled relevantnih standardov in smernic, primerjav praks ter oblikovanje vzorčnega delovnega protokola, je naloga dosegla zastavljen namen in pokaže, kaj loči zrel VOC od reaktivno organiziranega varnostnega nadzora ter kako te razlike vplivajo na odpornost organizacij.

Analiza kaže, da je osnovna struktura VOC v Evropi razmeroma poenotena. Operativno jedro tvorijo analitiki prve ravni (neprekinjen nadzor, *triage*, validacija dogodkov), druga raven vodi poglobljene tehnične preiskave in koordinira z nosilci infrastrukture, tretja raven pa izvaja lov na grožnje, digitalno forenziko in razvoj detekcij, prioritetno upravljanje zmogljivosti, merjenje uspešnosti in skrb za komunikacijske kanale z vodstvom, IT-operacijami in zunanjimi partnerji. Razlike med Slovenijo in najzrelejšimi evropskimi okolji izhajajo predvsem iz kadrovske širine, stopnje specializacije, uvedbe orkestracije in avtomatizacije, stalne pokritosti ter zrelih metrik. Kljub temu je v slovenskem prostoru opazen jasen trend profesionalizacije, standardizacije postopkov in približevanja najboljšim praksam.

Kljub intenzivni avtomatizaciji ostaja človeški faktor ključen. Kakovostna presoja konteksta, pravočasna komunikacija in odločanje pod časovnim pritiskom so področja, kjer algoritmi in pravila nujno potrebujejo kompetentne ljudi. Učinkovit VOC sistematično vlaga v razvoj veščin (tehničnih in mehkih), kulturo »po postopkih«, jasne vloge, redno rotacijo znanja ter inženiring detekcij. Pri tem so osrednjega pomena aktualna baza znanja, standardni operativni postopki in incidentni *playbooki*, ki zmanjšujejo variabilnost med izmenami in zagotavljajo ponovljivost odziva.

Operativna učinkovitost odzivanja v realnem času je pogojena s tremi prepletenimi sklopi: (1) kakovostno vidljivostjo (telemetrija iz SIEM/XDR/EDR/UEBA, dnevniški zapisi, mrežne sonde, CTI), (2) vnaprej definiranimi postopki z jasnimi pogoji eskalacije in vlogami ter (3) orkestracijo rutinskih korakov, ki analitikom prihranijo čas za presojanje in komunikacijo. Zreli

VOC poleg tega dosledno merijo uspešnost (MTTD, MTTR, kakovost *triage*, skladnost izvajanja *playbookov*) ter po vsakem pomembnejšem dogodku izvedejo pregled naučenih lekcij, posodobijo kontrole in okrepijo detekcije.

Regulativni okvir v Evropski uniji skupaj z nacionalnimi implementacijami VOC postavlja v vlogo operativnega nosilca skladnosti na področju kibernetske varnosti. Zahteve po pravočasnem poročanju, minimalnih tehnično-organizacijskih ukrepih, obvladovanju tveganj in neprekinjenem delovanju neposredno zahtevajo standardizirane postopke, sledljivost odločitev in dokumentirano komunikacijo z nacionalnimi pristojnimi organi in centri CSIRT. V slovenskem prostoru so večji in »bistveni« zavezanci naredili opazen napredek, medtem ko manjše organizacije in številni javni zavodi pospešeno uvajajo nadzorne zmogljivosti, formalizirajo procese in krepijo sodelovanje z zunanjimi izvajalci.

Upravljanje tveganj dobaviteljev se je izkazalo kot eden osrednjih praktičnih izzivov. Zrele prakse vključujejo pogodbeno urejene zahteve varnosti in poročanja, periodična vrednotenja dobaviteljev, omejevanje in segmentacijo dostopov, stalni nadzor vedenja tretjih strani ter posebne *playbooke* za incidente, ki izvirajo iz dobaviteljske verige. Sodelovanje z organi pregona, centri CSIRT in sektorskimi združenji je učinkovito predvsem, ko so komunikacijski protokoli, kontaktne točke in pravila izmenjave informacij (npr. TLP) vnaprej dogovorjeni in preizkušeni na vajah.

Pomemben praktični prispevek naloge je priprava vzorčnega delovnega protokola VOC, ki standardizira organizacijo izmen, operativne postopke, komunikacijske poti, preventivne kontrole, vodenje evidenc in povezavo z zahtevami standardov ter regulative. Tak protokol omogoča ponovljivost, sledljivost in primerljivost procesov, olajša uvajanje novih članov ter zmanjšuje odvisnost od neformalnega znanja posameznikov.

Na podlagi ugotovitev priporočamo: (i) dosledno formalizacijo postopkov in redne notranje presoje v okviru sistema upravljanja informacijske varnosti; (ii) postopno uvedbo SOAR za avtomatizacijo rutinskih opravil in orkestracijo odziva; (iii) celovit program metrik (MTTD/MTTR, stopnja lažnih pozitivnih, skladnost izvajanja *playbookov*); (iv) sistematično vlaganje v ljudi – specializacije za nivo 2/3, CTI in DFIR, strukturiran *onboarding* in mentorstvo; (v) redne tehnične in namizne vaje, ki preverjajo tako tehniko kot komunikacijo; (vi) okrepljeno upravljanje dobaviteljev z jasnimi pogoji, nadzorom dostopov in scenariji za incidente tretjih strani ter (vii) aktivno vključevanje v nacionalne in evropske mehanizme deljenja informacij in skupne vaje odpornosti. V prihodnje pričakujemo več konvergence XDR,

cloud-native nadzora, več proaktivnega *threat huntinga*, širšo uporabo analitike in umetne inteligence v podporo detekcijam ter hibridne modele delovanja v sodelovanju z zunanjimi partnerji.

Omejitve naloge izvirajo predvsem iz omejenega dostopa do zaupnih internih podatkov o delovanju posameznih VOC in iz dejstva, da primerjava zrelosti med sektorji in državami zajema heterogena okolja. Nadaljnje raziskave usmerjamo v kvantifikacijo učinkov avtomatizacije in formaliziranih *playbookov* na čas zaznave in odziva, v longitudinalne primerjave po sektorjih ter v ekonomsko-organizacijsko analizo različnih modelov.

Sklenemo lahko, da je VOC v sodobnih organizacijah osrednji nosilec operativne kibernetske varnosti. Njegova zrelost je neposredno odvisna od stopnje standardizacije, kompetenc ljudi, smiselne avtomatizacije in vpetosti v pravni in organizacijski okvir. V Sloveniji je viden pospešen premik k najboljšim evropskim praksam; jedro tega prehoda ostajajo dobro zasnovani procesi, merjenje uspešnosti, razvoj kadrov in premišljena tehnološka podpora.

11 LITERATURA IN VIRI

Zakon o gospodarskih družbah (ZGD-1). (14. april 2006). Pridobljeno iz pisrs.si: https://pisrs.si/pregledPredpisa?id=ZAKO4291

Zakon o informacijski varnosti (ZInfV). (17. april 2018). Pridobljeno iz Pisrs.si: https://pisrs.si/pregledPredpisa?id=ZAKO7707

Carrapico, H., & Barrinha, A. (1. februar 2018). *European Union cyber security as an emerging research and policy field.* Pridobljeno iz piblivations.aston.ac.uk: https://publications.aston.ac.uk/id/eprint/32413/1/European_Union_cyber_security_as_an_emerging_research_and_policy_field.pdf

Carrapico, H., & Barrinha, A. (1. februar 2018). *European Union cyber security as an emerging research and policy field.* Pridobljeno iz Taylor&Francis online: https://www.tandfonline.com/doi/epdf/10.1080/23745118.2018.1430712?needAccess=true

Cichnoski, P., Millar, T., Grance, T., & Scarfone, K. (avgust 2012). *Computer Security Incident Handling Guide.* Pridobljeno iz NIST.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cybersecurity Skills Academy. (brez datuma). Pridobljeno iz Digital Skills & Jobs Platform: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

Cybersecurity, E. U. (december 2024). *2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION.* Pridobljeno iz enisa.si: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf

De Zan, T., & Di Franco, F. (december 2019). *CYBERSECURITY SKILLS DEVELOPMENT IN THE EU.* Pridobljeno iz enisa.europa.eu: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20Skills%20Development%20in%20the%20EU.pdf

Direktiva 2022/2555. (14. december 2022). Pridobljeno iz eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022L2555

ENISA. (deceber 2020). *HOW TO SETUP UP CSIRT AND SOC.* Pridobljeno iz ENISA: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf

ENISA. (oktober 2023). *ENISA Threat Landscape 2023.* Pridobljeno iz European Union Agency for Cybersecurity: ENISA

ENISA. (juni 2023). *Good practices for supply chain cybersecurity.* Pridobljeno iz ENISA: https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf

ENISA. (december 2024). *2024 Report on the State of the Cybersecurity in the Union.* Pridobljeno iz Enisa.europa.eu: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

(2022). *ISO/IEC 27005:2022 Information security risk management. International Organization for Standardization.* International Organization for Standardization, ISO Central Secretariat. Geneva: ISO - Internetional Organization for Standardization.

Kajdiž, Z. (19. februar 2024). *Letno poročilo AJPES za leto 2023.* Pridobljeno iz ajpes.si: https://www.ajpes.si/Doc/AJPES/KIJZ/Letno_porocilo_AJPES_za_leto_2023_revidirano.pdf

Kathryn Knerler, I. P. (2024). *11 strategies of a world-class cybersecurity operations center.* Pridobljeno iz Mitre: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Scapicchio, M., Downie, A., & Finio, M. (15. marec 2024). *What is a SOC?* Pridobljeno iz ibm.com: https://www.ibm.com/think/topics/security-operations-center

SI-CERT, N. o. (2024). *Pročilo o kibernetski varnosti 2023.* Pridobljeno iz cert.si: https://www.cert.si/wp-content/uploads/2024/05/Porocilo-o-kibernetski-varnosti_2023_SI-CERT_web.pdf

Slovenija, T. (brez datuma). *Center Kibernetske varnosti in Odpornosti*. Pridobljeno iz Telekom Slovenije: https://www.telekom.si/veleprodaja/domaca-veleprodaja/center-kibernetske-varnosti-in-odpornosti-ckvo?utm_source=chatgpt.com

Unistar LC d.o.o. (29. maj 2025). *Ko varnost postane strateški temlj poslovanja*. Pridobljeno iz Računalniške novice: https://racunalniske-novice.com/ko-varnost-postane-strateski-temelj-poslovanja/

Urad Vlade Republike Slovenije za informacijsko varnost. (23. maj 2025). *Zakon o informacijski varnosti (ZInfV-1).* Pridobljeno iz pisrs.si: https://pisrs.si/pregledPredpisa?id=ZAKO8934

Uradni list Evropske unije. (14. december 2022). *DIREKTIVE.* Pridobljeno iz European Commission: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022L2555

UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA . (14. december 2022). Pridobljeno 2025. avgust 30 iz eu-lex.europa.eu: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022R2554

UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA. (14. december 2022). Pridobljeno 2025. avgust 30 iz eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022R2554

12 PRILOGE

Priloga 1: Vzorec delovnega protokola za varnostno-operativni center