УНИВЕРЗИТЕТ У НОВОМ САДУ

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

РАЗВОЈ БЕЗБЕДНЕ МИКРОСЕРВИСНЕ АРХИТЕКТУРЕ У КРИТИЧНИМ ИНФРАСТРУКТУРНИМ СИСТЕМИМА

ДОКТОРСКА ДИСЕРТАЦИЈА

Ментори:
Проф. др Дарко Чапко
Проф. др Имре Лендак

Кандидат:
Марина Станојевић

Нови Сад, 2024. године

УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА **ОБРАЗАЦ – 5а**

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА[1]

Врста рада:	Докторска дисертација
Име и презиме аутора:	Марина Станојевић
Ментор (титула, име, презиме, звање, институција):	Проф. др Дарко Чапко, редовни професор, Факултет техничких наука, Универзитет у Новом Саду Проф. др Имре Лендак, ванредни професор, Факултет техничких наука, Универзитет у Новом Саду
Наслов рада:	Развој безбедне микросервисне архитектуре у критичним инфраструктурним системима
Језик и писмо рада:	Српски, ћирилица
Физички опис рада:	Унети број: Страница 96 Поглавља 6 Референци 102 Табела 8 Слика 15 Графикона / Прилога 5
Научна област:	Електротехничко и рачунарско инжењерство
Ужа научна област (научна дисциплина):	Примењено софтверско инжењерство
Кључне речи / предметна одредница:	Микросервисна архитектура, рачунарство у облаку, сигурност, безбедност, принцип нултог поверења, критичне инфраструктуре
Апстракт на језику рада:	Ова докторска дисертација се бави истраживањем које је везано за безбедност критичних инфраструктуа. У савременом добу од ових система се очекује да прате тренд повећане потражње што је могуће само њиховом адаптацијом на нове технологије. Нове технологије доносе и нове безбедносне ризике који морају бити адресирани у системима овог нивоа критичности. Отказ система, крађа информација и слично могу довести до катастрофалнх последица као што је губитак људских живота, негативан утицај на животну средину, велики финансијски губици и слично. Препознато је да коришћењем микросервисне архитектуре и рачунарства у облаку ови системи могу да одговоре на потребе њихових корисника. Као резултат истраживања архитектуре, аутор је дошао до закључка да принципи нултог поверења, одране у дубину, принцип најмањих привилегија као и коришћење компоненти облака значајно доприносе безбедности описаних система како од екстерних нападача тако и од инсајдера. У дисертацији је предложена и презентована архитектура која имплементира споменуте принципе након извршене анализе рањивости над референтним системом. Као доказ о

[1] Аутор докторске дисертације потписао је и приложио следеће Обрасце:
5б – Изјава о ауторству;
5в – Изјава о истоветности штампане и електронске верзије докторског рада и дозвола за објављивање личних података;
5г – Изјава о коришћењу.
Ове Изјаве се чувају у институцији у штампаном и електронском облику и не кориче се са радом.

	подобности архитектуре спроведена је анализа безбедности компоненти референтног система користећи STRIDE методологију где је показано да су ризици рањивости ниски. Као резултат дисертације, поред предложених безбедносних мера, презентовани су и нефункционални безбедносни захтеви за ове системе као и процес анализе рањивости који је био почетни корак у истраживању.
Датум прихватања теме од стране надлежног већа:	30.11.2023.
Датум одбране: (Попуњава накнадно институција)	
Чланови комисије: (титула, име, презиме, звање, институција)	Председник: др Срђан Вукмировић, редовни професор, Факултет техничких наука, Нови Сад Члан: др Јелица Протић, редовни професор, Електротехнички факултет, Београд Члан: др Себастијан Стоја, доцент, Факултет техничких наука, Нови Сад Члан: др Дарко Чапко, редовни професор, Факултет техничких наука, Нови Сад Члан: др Имре Лендак, ванредни професор, Факултет техничких наука, Нови Сад
Напомена:	

UNIVERSITY OF NOVI SAD
FACULTY OF TECHNICAL SCIENCES

KEY WORD DOCUMENTATION[2]

Document type:	Doctoral dissertation
Author:	Marina Stanojević
Supervisor (title, first name, last name, position, institution)	Darko Čapko, Phd, Full Professor, Faculty of Technical Sciences, University of Novi Sad Imre Lendak, Phd, Associate Professor, Faculty of Technical Sciences, University of Novi Sad
Thesis title in English:	Development of secure microservice architecture in mission critical systems
Language and script:	Serbian language, cyrillic script
Physical description:	Number of: Pages 96 Chapters 6 References 102 Tables 8 Illustrations 15 Graphs / Appendices 5
Scientific field:	Electrical and computer engineering
Scientific subfield (scientific discipline):	Applied software engineering
Subject, Key words:	Microservice architecture, cloud computing, security, safety, zero trust model, critical infrastructure.
Abstract in English:	This doctoral dissertation addresses research related to the security of critical infrastructure systems. In the modern era, these systems are expected to keep up with the increasing demand, which is only possible through their adaptation to new technologies. However, new technologies bring new security risks that must be addressed in systems of this level of criticality. System failure, data theft, and similar incidents can lead to catastrophic consequences such as loss of human life, negative environmental impacts, significant financial losses, and more. It has been recognized that by utilizing microservice architecture and cloud computing, these systems can meet the needs of their users. As a result of the research into the architecture, the author concluded that the principles of zero trust, defense in depth, the principle of least privilege, and the use of cloud components significantly contribute to the security of these systems, protecting them from both external attackers and insiders. The dissertation proposes and presents an architecture that implements these principles following a threat analysis conducted on the reference system. To prove the suitability of the architecture, a security analysis of the reference system's components was performed using the STRIDE methodology, demonstrating that the risks of identified threats are low. As a result of the dissertation, in addition to the proposed security measures, non-functional security requirements for these systems are

[2] The author of the doctoral dissertation has signed the following Statements:
5б – Statement on the authorship,
5в – Statement that the printed and e-version of the doctoral dissertation are identical and authorization to use personal data,
5г – Copyright statement.
The paper and e-versions of Statements are held at the institution and are not included into the printed thesis.

	presented, along with the threat analysis process, which was the initial step in the research.
Date of endorsement by the scientific board:	30.11.2023.
Date of defence: (Filled in by the institution)	
Thesis defence board: (title, first name, last name, position, institution)	Chair: PhD Srđan Vukmirović, Full Professor, Faculty of Technical Sciences, Novi Sad Member: PhD Jelica Protić, Full Professor, Faculty of Elecrical Engineering, Belgrade Member: PhD Sebastijan Stoja, Assistant Professor, Faculty of Technical Sciences, Novi Sad Member: PhD Darko Čapko, Full Professor, Faculty of Technical Sciences, Novi Sad Member: PhD Imre Lendak, Associate Professor, Faculty of Technical Sciences, Novi Sad
Note:	

Захвалница

Пре свих, захвалност дугујем својим менторима, Дарку и Имрету. Заиста је велика привилегија и част бити ваш докторант. Много сам захвална што сам имала прилику да учим од вас и што сте ме баш ви водили кроз овај пут, као велики стручњаци у овој изазовној области. Хвала Вам што сте веровали у мене, за сваку реч мотивације, за несебично дељење знања и усмеравање. Ова дисертација не би била написана без ваше подршке и помоћи. Иако то нису званично, као своје менторе доживљавам и Себастијана и Бојана. Хвала вам за сваку реч подршке, мотивације, савета.

Моја породица је моја највећа снага. Безусловна подршка, љубав и усмеравање кроз цео живот су нас довели до овог момента. Хвала вам што смо једно. Ова дисертација је ваша.

Куми Александри се захваљујем што је увек ту за мене, да саслуша и помогне. Јелени што смо овај пут пролазиле заједно, што ме разуме, даје савете и ветар у леђа.

Хвала свим професорима, пријатељима и колегама на подршци, мотивисању, сарадњи. Свака реч је значила.

На овом путу никада нисам била сама, увек сам имала коме да се обратим за помоћ и подршку. Хвала вам што сте мој тим, што сте ме увек гурали напред!

САДРЖАЈ

СПИСАК КОРИШЋЕНИХ СКРАЋЕНИЦА

Скраћеница	***Пуни назив***
ЕУ	*Европска унија*
EPCIP	*European Programme for Critical Infrastructure Protection*
GAO	*Government Accountability Office*
IT	*Information Technology*
OT	*Operational Technology*
ИКС	*Индустријски контролни системи*
RTU	*Remote terminal unit*
SCADA	*Supervisory control and data acquisition*
DCS	*Distributed control system*
HMI	*Human machine interface*
PLC	*Programmable Logic Controller*
DNP3	*Distributed Network Protocol 3*
IoT	*Internet-of-Things*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
IDPS	*Intrusion detection and prevention system*
OWASP	*Open Web Application Security Project*
ISO/IEC	*International Organization for Standardization*
IACS	*Industrial automation and control systems*
ISA/IEC	*International Society of Automation*
PII	*Personally Identifiable Information*
NERC CIP	*North American Electric Reliability Corporation – Critical Infrastructure Protection*
NIST	*National Institute for Standards and Technology*

CSA	*Cloud Security Aliance*
SOC 2	*Service Organization Control 2*
AICPA	*American Institute of Certified Public Accountants*
IaaS	*Infrastructure as a Service*
PaaS	*Platform as a Service*
SaaS	*Infrastructure as a Service*
ENISA	*European Union Agency for Cybersecurity*
GDPR	*General Data Protection Regulation*
NIS	*Directive on security of network and information systems*
CCM	*Cloud Controls Matrix*
AWS	*Amazon Web Services*
CIS	*Center for Internet Security*
CIA	*Confidentially, Integrity, Availability*
DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
IP	*Internet Protocol*
MS	*Сервис за размену порука*
DS	*Сервис динамике*
RD	*База података у реалном времену*
HD	*Историјска база података*
MDS	*Сервис за управљање статичким моделом*
OMS	*Сервис за управљање прекидима*
SMS	*Сервис управљања поправкама*
AF	*Аналитичка функција*
HIST	*Сервис за приступ историјској бази података*
INT	*Сервис за интеграције*
SMMS	*Сервис за управљање паметним бројилима*
ОС	*Оперативни систем*
TCP	*Transmission Control Protocol*
CRC	*Cyclic redundancy check*
ICCP	*Inter-Control Center Communications Protocol*
SQL	*Structured Query Language*
VPN	*Virtual Private Network*

MitM	*Man In the Middle*
OIDC	*OpenID Connect*
OAuth2.0	*Open Authorization* protocol
JIT	*Just-In-Time*
IdP	*Identity Provider*
JWT	*JSON Web Token*
MFA	*Multi-factor Authentication*
RBAC	*Role-based access control*
SIEM	*Security Information and Event Management*
ACL	*Access control lists*
DPI	*Deep Packet Inspection*
RLS	*Row Level Security*
APT	*Advanced persistent threats*
CPU	*Central Processing Unit*
SOAR	*Security orchestration, automation and response*
SOC	*Security Operations Center*
CA	*Certificate Authority*
SSL	*Secure Sockets Layer*
WAF	*Web Application Firewall*
TLS	*Transport Layer Security*
STRIDE	*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*
JSON	*JavaScript Object Notation*
SSO	*Single Sign-On*
PKI	*Public Key Infrastructure*
SHA	*Secure Hash Algorithm*
PKCE	*Proof Key for Code Exchange*
DNS	*Domain Name Server*
CDM	*Continuous diagnostics and mitigation*
PEP	*Policy enforcement point*
PA	*Policy administrator*
PE	*Policy engine*
PDP	*Policy Decision Point*

СПИСАК СЛИКА

СПИСАК ТАБЕЛА

1. УВОД

Са развојем рачунарства и дигитализације која уводи рачунарске системе у свакодневни рад и живот човека, изложеност поверљивих информација малициозним актерима никада није била већа. Сајбер криминал је у последњој деценији у порасту и нападачи покушавају на разне начине да искористе рањивости система. Постоји више врста нападача па самим тим и мотив за напад може бити различит. Циљ напада може бити дискредитовање конкуренције, где ће се њихов систем показати као непоуздан, што доводи до губитка клијената и новца. У том случају, нападач је компанија, па чак и држава. Други тип нападача је индивидуалац који има жељу за осветом, новцем или само да покаже своје способности. У већини напада учествују такозвани инсајдери, запослени, или бивши запослени компаније, који има приступ систему као и знање о његовим рањивостима што значајно олакшава извођење напада.

По дефиницији Европске комисије, критична инфраструктура представља средство, систем или његов део који се налази у државама чланицама Европске Уније (ЕУ), а који је неопходан за одржавање виталних друштвених функција, здравља, безбедности, сигурности, економског или социјалног благостања људи, а чији би прекид у раду или уништење имало значајан утицај у држави чланици као резултат неспособности одржавања тих функција [1]. Европска комисија већ дуже време активно подржава заштиту критичне инфраструктуре и отпорност кључних ентитета на природне и ризике које уводи човек. Путем Европског програма за заштиту критичне инфраструктуре (енг. *European Programme for Critical Infrastructure Protection,* EPCIP) предложена је директива [2] која има за циљ да учврсти отпорност кључних ентитета на различите претње, укључујући природне непогоде, терористичке нападе, унутрашње претње или саботажу, као и ванредне ситуације јавног здравља. По NIS 2 директиви [3] следећих 15 сектора се сматрају критичним у ЕУ: енергетски сектор, здравство, транспорт, финансије, пијаћа вода, дигитална инфраструктура, јавна управа, дигитални провајдери, пошта, управљање отпадом, свемирски сектор, сектор производње, прераде и дистрибуције хране, производња, хемијски и истраживачки сектор.

Government Accountability Office (GAO) у свом истраживању [4] наводи све системе који су од критичног значаја за САД. То су следећих 16 сектора: хемијски сектор, сектор комерцијалних објеката, комуникациони сектор, сектор критичне производње, сектор брана, сектор хитних служби, сектор информационих технологија, сектор нуклеарних реактора, материјала и отпада, сектор државних објеката, сектор транспортних система, сектор одбрамбене индустрије, енергетски сектор, сектор финансијских услуга, сектор за храну и пољопривреду, сектор здравства и јавног здравља и сектор вода и отпадних вода. Критичне инфраструктуре се састоје из ИТ система предузећа и система оперативне технологије. Због њихове сложености и потребе да комуницирају са другим системима они су рањиви на разне врсте сајбер напада [5]. Ови системи морају да буду поуздани, да

буду заштићени од злонамерних активности, да одрже свој интегритет и доступност тако да је безбедност од кључне важности за њих. Успешни напади на критичне инфраструктуре могу угрозити безбедност и сигурност људи, окружење као и економију.

Индустријски контролни системи (ИКС) надгледају и контролишу процесе у критичним инфраструктурама [6]. Ови системи користе комуникационе канале за повезивање контролног центра са удаљеним подстаницама. Удаљени терминални уређаји (енг. *Remote terminal unit*, RTU), који се користе у подстаницама, комуницирају са сензорима за праћење статуса и пренос података контролном центру, као и актуаторима који извршавају контролне акције на основу команде из контролног центра. Безбедност ових система захтева интегрисани приступ који обухвата техничке, организационе и процедуралне мере. Редовно ажурирање и тестирање сигурносних полиса, имплементација најбољих пракси безбедности и стално праћење и ажурирање система су кључни кораци ка обезбеђивању интегритета и поузданости.

Коришћење микросервисне архитектуре као платформе даје могућност аутоматског скалирања сервиса где се при повећаној потражњи повећава и број инстанци сервиса. Поред тога, уводи се редундантност сервиса па самим тим и повећава отпорност на отказе. Мана ове архитектуре у односу на монолитну је то што се поделом система на више сервиса уводи потреба за комуникацијом између њих која постаје уско грло и чини систем рањивијим са аспекта безбедности.

1.1 Мотивација и дефинисање проблема

За модерно друштво, заштита критичне инфраструктуре и отпорност кључних ентитета који управљају том инфраструктуром је витална. Без поузданих извора енергије, безбедне воде за пиће, здравствених услуга, банкарских и финансијских услуга или предвидљивог транспорта, између осталих, начин живота као што га познајемо не би био могућ [7]. Критичне инфраструктурне морају да имају одзив у реалном времену, чији отказ може да угрози људски живот као и да произведе високе финансијске губитке. Због природе ових система, они се најчешће налазе у изолованим рачунарским центрима где је сигурност на високом нивоу. Нема дилеме да је безбедност ових система јако битна, међутим, поред тога битно је и испратити нове захтеве тржишта и бити стално у корак са њима. Количина, проток и обрада информација се стално повећава па самим тим мора и технологија да напредује како би се захтеви испратили.

У последње две деценије, ИКС су трансформисани и унапређени од власничке и изоловане архитектуре до отворене и стандардне платформе, која је повезана са корпоративним мрежама [8]. Овај развој је отворио нове могућности (попут даљинског приступа мрежама и уређајима), али је такође учинио ИКС рањивим на широк спектар сајбер напада. Предмет напада није само политика и процедуре безбедности, већ и хардвер, софтвер, платформа и рањивости мреже ИКС. Напади на ИКС нису новост. Према извештају из Kaspersky, 1997. године су објављене само две рањивости. Међутим, овај индекс је порастао на 19 у 2010. години. Од тада, број рањивости значајно расте, па је 2015. године откривено 189 рањивости у ИКС. Како се број ИКС доступних преко интернета повећава сваке године, од кључног је значаја да ИКС администратори буду свесни нових рањивости и активно побољшавају безбедност својих.

Енергетска индустрија у последњој деценији постала је једна од главних мета нападача. Smart Grid OT је систем чија је главна сврха надгледање дистрибутивне мреже. Садржи приказан статус опреме која је на терену у реалном времену, омогућава командовање том опремом као и помоћ приликом пријаве инцидената на дистрибутивној мрежи и отклањања кварова. Систем мора да буде доступан 24 сата при чему мора брзо да обрађује информације којима располаже. Сматра се критичним јер грешка у његовом раду може да проузрокује огромну штету па чак и да угрози људске животе. Из наведених разлога, годинама уназад, Smart Grid OT је био инсталиран у обезбеђеним рачунарским центрима електродистрибуција, ослањајући се на монолитну, сервисно-оријентисану архитектуру. Потражња за електричном енергијом је у све већем порасту, па се човечанство окреће обновљивим изворима енергије. Smart Grid OT систем да би могао да подржи ове промене, потребно је увођење нових компоненти и прелазак на нове технологије. Микросервисна архитектура и рачунарски облак су добро решење када је у питању решавање проблема скалабилности, перформанси и одзива система [9]. Како би се предности микросервисне архитектуре могле искористити у критичним инфраструктурама, потребно је анализирати претње над системом у циљу прављења безбедне архитектуре што је и тема ове докторске дисертације.

Развој безбедне архитектуре микросервисних система је процес који може бити примењен како у критичним инфраструктурама тако и у другим системима. Процес узраде безбедне архитектуре критичних инфраструктура креће од анализе захтева које тај систем треба да задовољи. Потребно је дефинисати компоненте система, јасне границе између њих, токове података и тачке улаза/излаза у систем. За измоделовани систем се прави модел претњи. Након генерисања извештаја, предлаже се нова архитектура система у којој је уграђена безбедност и где је акценат на смањењу вероватноће да се нађене рањивости експлоатишу. Резултат ове докторске дисертације доказује да је могуће имплементирати и користити предности модерне технологије у критичним инфраструктурама и у исто време задржати потребан ниво безбедности.

1.2 Хипотезе и циљеви истраживања

У наставку су наведене хипотезе ове докторске дисертације:

- **X1**: Могућ је развој безбедне архитектуре индустријског контролног система базираног на микросервисима у рачунарском облаку.
- **X2**: Принцип нултог поверења је применљив у индустријским контролним системима.
- **X3**: STRIDE методологија за анализу ризика је применљива и у контексту развоја модерних индустријских контролних система са микросервисном архитектуром.

Примарни циљеви истраживања су изведени из претходно дефинисаних хипотеза. Први очекивани резултат је дефинисан скуп безбедносних мера које морају бити имплементиране у архитектури критичне инфраструктуре како би се смањио ризик од напада. Као референтни систем над којим ће бити тестирана предложена архитектура је изабран OT систем имплементиран на микросервисној архитектури који је постављен у рачунарском облаку. Други резултат је списак нефункционалних безбедносних захтева које референтни систем мора да задовољи.

1.3 Приказ дисертације по поглављима

Уводно Поглавље 1, садржи описан мотив за писање ове докторске дисертације. Дат је кратак опис проблема који се решава и на крају дефинисане хипотезе и циљеви.

У оквиру Поглавља 2, дат је теоријски увод и актуелно стање у области које су истраживане у докторској дисертацији. Садржи опис критичних инфраструктура, изазове у њиховој безбедности, микросервисну архитектуру, спој микросервисне архитектуре, рачунарства у облаку и како модел нултог поверења може да помогне у постизању безбедности микросервиса. На крају и шта то подразумева безбедна архитектура, које су кључне безбедносне основе и како тестирати безбедност система.

У Поглављу 3 је описан изабран референти систем, његова архитектура, компоненте и токови података између њих. Поред тога је описан процес анализе ризика над ИКС, извршена анализа претњи над архитектуром предложеног референтног система и дефинисан модел претњи.

У оквиру Поглавља 4, дат је предлог безбедне архитектуре система као и скуп сигурносних мера који морају бити задовољене како би се вероватноћа експлоатисања нађених претњи смањила. Описани су и нефункционални безбедносни захтеви за критичне инфраструктуре.

Поглавље 5 садржи имплементацију *STRIDE* методологије над предложеном безбедном архитектуром као и резултате ове анализе. Што уједно представља валидацију архитектуре и нефункционалних безбедносних захтева.

У поглављу 8 је приказан закључак докторске дисертације са наведеним могућим правцима даљег истраживања.

2. ТЕОРИЈСКЕ ОСНОВЕ

У савременом дигиталном свету, развој микросервисних система представља значајан напредак у начину на који се софтвер развија, доставља и одржава. Ова архитектура омогућава флексибилност, скалабилност и брзину у развоју апликација, што представља значајану предност у модерном програмирању. Међутим, са овим напретком долазе и нови изазови у области безбедности [10]. Микросервисна архитектура и облак решавају проблеме скалабилности, перформанси и одзива система [9] и као такви представљају логичан правац напретка за унапређење архитектуре ИКС. Како се применом нових технологија наслеђују и њихове рањивости, у овом поглављу, истражује се тренутно стање безбедности микросервисне архитектуре, рачунарства у облаку и познате рањивости и механизми заштите ИКС. Недавна истраживања показују да је претња над ИКС знатно виша него што је очекивано и то доводи у опасност и озбиљан ризик јавну безбедност, заштиту средине и финансије. Сајбер напади над овим системима се дешавају у великој мери, на пример у 2014 години одговорено је на 245 инцидента [11]. Тренутно стање што се тиче покушаја напада је још горе, 2023. године је забележено више од 420 милиона напада што би значило да се сваке секунде деси 13 напада [12].

Успешност напада зависи од мотива, знања и спретности нападача. Постоје групе малициозних актера који представљају претњу на критичне инфраструктуре. Ови актери по GAO [5] се деле на следеће групе:

- Државе – укључује државе, нације, групе или програме које подржава држава. Они користе нападе како би испунили неки економски, војни или политички циљ.
- Транснационалне криминалне групе – укључујући и организоване криминалне групе. Користе нападе како би дошле до новца.
- Хакери и хактивисти – врше упаде у мреже из више разлога као на пример испуњење неког изазова, освете, ухођење или због новчане добити. Насупрот томе, хактивисти су идеолошки мотивисани и они користе алате за сајбер нападе за постизање политичких циљева.
- Инсајдери – појединци (као што су запослени, уговарачи или продавци) који имају овлашћен приступ систему или предузећу и могућност да намерно или несвесно нанесе штету.

2.1 Индустријски контролни системи

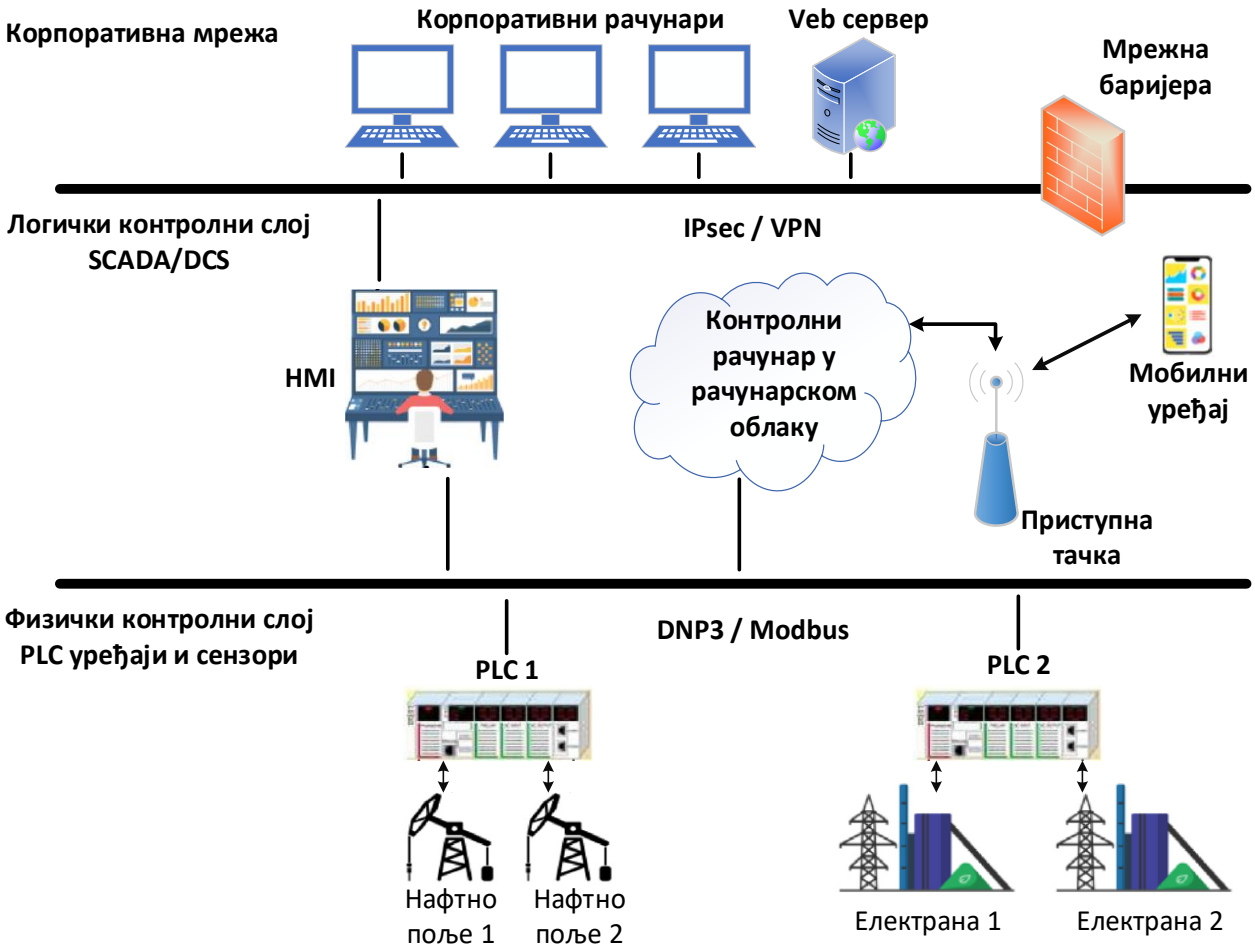
ИКС садржи скуп елемената укључујући технологије, машине, људске факторе, физичке процесе и системе који међусобно интерагују. Безбедносни ризици на ИКС потичу најчешће од људских фактора или од техничких рањивости. Постизање адекватне безбедности за ИКС захтева истраживање и имплементирање разних безбедносних

области, на пример, рачунарску безбедност, безбедност комуникација, оперативну безбедност и физичку безбедност. Интеграција ових безбедносних специјалности доприноси постизању безбедног система са високим степеном поверења. Као хијерархијски систем, ИКС је формиран са комплексним и вишеслојним индустријским мрежама са многим повезаним компонентама, уређајима и подсистемима који заједно раде на одржавању мерења и контроле индустријских процеса. Стога, проблем у безбедности ИКС није само на везама између компоненти контролног система већ и на интерконекцијама са другим мрежама, самим системом и опремом, као и на индустријским процесима. На слици 1 је представљен преглед системске архитектуре ИКС која се може поделити на три слоја [8]:

1. На слоју **корпоративне мреже**, менаџери могу приступити ИТ систему.

2. У слоју **логичке контроле** (SCADA/DCS), систем администратори користе интерфејс човек-машина (енг. *human machine interface*, HMI) или надзорни рачунар у облаку за праћење статуса производње и слање команди за ажурирање контролне секвенце.

3. Сви контролни уређаји (нпр. PLC и сензори), протоколи (нпр. DNP3/Modbus) и производни објекти категорисани су као **физички контролни** слој.



Слика 1 - Преглед ИКС инфрастуктуре [8]

2.1.1 Изазови у безбедности

У прошлости се није пуно пажње придавало безбедности ИКС јер се сматрало да је довољно то што су изоловани [11]. Неколико сајбер напада се десило последњих година што је срушило мит о изолацији и подигнуло проблем безбедности ИКС на виши ниво [11, 13, 14, 15, 16, 17, 18, 19]. Нападачи активно прате рањивости нултог дана (енг. *zero-day*) у софтверу и хардверу, што додатно усложњава задатак оператерима обезбеђивања ИКС која би требало да буде укорењена у фундаменталним захтевима и уграђена у архитектуру ИКС [20, 21]. У табели испод су приказане четири димензије које представљају разлог зашто постаје све теже постићи жељени ниво безбедности ИКС.

Табела 1 – Четири главне категорије безбедносних проблема у ИКС [9]

Индустријски контролни систем	
Напредак технологија	**Развој система**
Рачунарство у облаку Велики подаци Технологија мрежа Микропроцесори	Изолован -> отворен Повећана интерконективност Адаптација ИТ решења Комерцијална доступност .....
Еволуција образаца напада	**Фактори управљања**
Напредне технике напада Разноликост претњи Интелигентни напад Чешћи напади	Ниска свест о безбедности Недостаци у управљању Недостаци у дизајну Нарушено функционисање током рада .....

Увођењем нових технологија и интеграција у критичне инфраструктуре долази до повећања ризика како за спољашње тако и унутрашње нападе [22]. Следеће рањивости се испољавају:

- ***Рањивости архитектуре*** – слаба сепарација између IT и OT мрежа. Недостаје аутентификација у комуникацији активних компоненти (нпр. између актуатора и SCADA сервера, актуатора и RTU уређаја и слично). Недостајање безбедносних механизама који обезбеђују интегритет команди које се размењују. Мрежна баријера (енг. *firewall*) је једина тачка квара (енг. *The single point of failure*).
- ***Рањивости безбедносне полисе*** – примењене безбедносне полисе морају бити унапређене, посебно оне које се односе на удаљени приступ корисника. Поред тога, полисе за праћење приступа и активности на систему морају бити јасно дефинисане.
- ***Рањивости софтвера*** – у погледу оперативних система, ситуација је врло хетерогена где се користи велики број различитих оперативних система. Рањивост може бити и у застарелим верзијама оперативног система, као и апликација које су инсталиране на рачунарима.

Због претпоставке да је изолација довољна из угла безбедности, многи индустријски комуникациони протоколи, укључујући Modbus и Distributed Network Protocol 3 (DNP3),

нису имали основне безбедносне функције за обезбеђивање порекла или свежине пакета података. Такође, заштита граница зона није добила довољно пажње. У SCADA систему, удаљен приступ са слабом аутентификацијом може бити лако злоупотребљен од стране нападача.

Нападачи користе рањивости хардвера и софтвера како би унели измене које доводе до одступања од нормалног понашања система [23]. Грешке које настају као последица ових активности се класификују као ***интерне*** и ***спољашње***. Интерна грешка одговара неауторизованим променама унутар система. Спољашње грешке потичу изван система и могу бити природне појаве, злонамерне радње или несреће. Без обзира на узрок, грешка може изазвати интерни системски проблем који може утицати на пружање основних услуга и извршавање контролних радњи. На пример, напад на сензорски чвор може изазвати хардверске или софтверске грешке које могу утицати на рад других неопходних контролних ресурса као што су удаљени RTU уређаји. Ако се ово деси, контролни центар може бити спречен да прими виталне информације из подстаница и тако постаје слеп за стварно стање система којим се управља. Ова ситуација такође може настати када комуникационе везе престану са радом или када су компромитоване од стране злонамерних ентитета.

Постоје две категорије извора сајбер претњи, ***унутрашње*** и ***спољашње***. Главни извори унутрашњих претњи су углавном незадовољни запослени. Спољашње претње укључују хакере и криминалне групе. Иако 85% штете долази од инсајдера [24] који могу бити запослени или трећа страна од поверења са одговарајућим привилегијама (нпр. добављач), већина студија покрива заштиту од напада који долазе од спољних претњи. Први корак за побољшање одбране од инсајдера је успостављање јаких безбедносних полиса и стално праћење активности запослених [25]. Један од начина да се приступи бољем разумевању инсајдерске претње је идентификовање опсега проблема, техничких и бихевиоралних догађаја и индикатора као и анализа потенцијалних нападача и њихове мотивације [26]. Референца [27] извештава о сличним истраживањима са фокусом на окружења интернета ствари (енг. *Internet-of-Things,* IoT*).* Аутори референце [28] анализирали су 120 стварних студија случаја и дефинисали обрасце напада који би могли да помогну у откривању инсајдерских претњи. Анализа инсајдерских претњи и заштита од њих је представљена у раду [29] где се као решење наводи коришћење принципа и архитектуре нултог поверења (описано у додатку Ц).

Нове технологије унапређују ИКС у смислу функционалности и практичности, међутим повезаност ових система са интернетом уводи ризик од различитих сајбер претњи [9]. Нападачи могу да искористе везу са интернетом, посебно ако се користе слабо заштићене или незаштићене бежичне приступне тачаке како би компровитовали контролне системе и добили приступ мрежи или уређајима. Након тога могу убацити лажне контролне команде и мерене вредности, па чак и блокирати комуникационе канале. Да би се компромитовало управљање ИКС, како изнутра тако и изван њих, нападачи углавном изводе део или све кораке [30]:

1. ***Извиђање*** путем друштвеног инжењерства (енг. *social engineering*) или других метода нападач прикупља информације.

2. ***Наоружавање*** тражењем рањивости система, уређаја или запослених како би се могао инсталирати малициозан софтвер.

3. ***Достављање*** малициозног софтвера преко интернета, поруке, USB диска и слично.

4. ***Искоришћавање рањивости*** како би се малициозни софтвер инсталирао.

5. ***Инсталација*** малициозног софтвера на више сервера. Ово омогућава нападачу да задржи приступ систему чак и када је откривен и да се несметано враћа и извршава малициозне радње.

6. Обезбеђен је удаљен приступ након чега следи ***командовање и контрола*** системом**.**

7. Извршено је све потребно како би нападач ***остварио циљ*** напада. То може бити крађа осетљивих информација, ометање пословних операција, захтевање откупа или друге злонамерне активности.

Рачунарство у облаку може помоћи у заштити критичне инфраструктуре [32]. Рачунарство у облаку обезбеђује неколико оперативних бенефита, укључујући редунданцију података, доступност података и опстанак (када су есенцијалне компоненте система изоловане или изгубљене). На пример, уколико контролни центар изгуби своје оперативне услуге, други контролни центар у рачунарском облаку би могао преузети контролу. Рачунарство у облаку може олакшати развој индустријских апликација које подржавају интероперабилност и сарадњу између организација и ентитета. Механизми безбедности и приватности морају бити имплементирани укључујући криптографске шеме, аутентификацију и управљање идентитетом, контролу приступа, као и управљање поверењем, управљање, полисе и регулативе. Редунданцију података у рачунарству у облаку такође треба пажљиво разматрати заједно са детекцијом упада, алармима и руковањем инцидентима.

2.1.2 Безбедносне мере за заштиту ИКС

Сигурност у пракси се одређује степеном примене безбедносних мера (контрола) на све три компоненте ИКС (људе, процесе и технологију) како би се одржала поузданост и континуитет операција [31]. Треба посветити пажњу и физичкој безбедности, односно сигурности уређаја који су саставни део ИКС (подстанице, трансформатори, сензори, и сл.). Мере које се предузимају како би се постигла физичка сигурност компоненти ИКС су ограде, баријере, чувари, патроле, заштићене капије и врата, сигурносне браве, аларми, камере, сензори за детекцију покрета итд. На пољу физичке безбедности опреме, мере заштите укључују усаглашеност са безбедносним стандардима, редовне инспекције и одржавање, обуку и сертификацију особља, безбедносне функције и међузакључавања, технике за уземљење и изолацију, безбедносне ознаке и етикетирање, планове за хитне интервенције, усаглашеност са прописима о заштити на раду, механизме за откривање кварова и заштиту, системе за превенцију и сузбијање пожара, праћење животне средине [32]. Ове мере обезбеђују сигуран рад опреме, минимизирају ризик од несрећа и штите како особље, тако и осигуравају поуздан рад система. Мере за осигуравање безбедности за ИКС су следеће [6]:

- ***Методологије за процену ризика***: Спровођење процене ризика сајбер и физичке безбедности је битно ради идентификације рањивости и потенцијалних претњи у окружењима ИКС. Методологије процене ризика помажу организацијама да

разумеју потенцијални утицај напада и да према томе приоритетно распоређују мере безбедности.

- ***Контрола приступа***: Примена мера контроле приступа је кључна за заштиту ИКС. Ово укључује механизме аутентификације како би се осигурало да само овлашћене особе могу приступити систему. Контрола приступа такође подразумева дефинисање улога и дозвола корисника како би се ограничио приступ осетљивим областима ИКС.
- ***Откривање и превенција упада***: Систем за откривање упада (енг. *Intrusion Detection System*, IDS) је важан за праћење активности у ИКС и откривање било каквог злонамерног понашања. IDS може помоћи у идентификацији потенцијалних сајбер напада и активира аларма за хитну реакцију. Системи за превенцију упада (енг. *Intrusion Prevention System*, IPS) могу се такође имплементирати како би активно блокирали или ублажили нападе. Ови системи се ретко користе у ИКС јер уносе ризик због прекида легитимног саобраћаја.
- ***Енкриптовање података***: Техника енкриптовања података се користи ради заштите осетљивих информација које се преносе између различитих компоненти ИКС. Енкриптовање осигурава да подаци остану поверљиви и да их неовлашћене особе не могу пресрести или изменити.
- ***Модели за процену безбедности***: Користе се ради оцењивања ефикасности мера безбедности примењених у ИКС. Ови модели помажу организацијама да идентификују слабости или празнине у својој безбедносној инфраструктури и донесу одлуке о побољшању безбедности.
- ***Политике и смернице за безбедност***: Важан је развој и примена безбедносних политика и смерница специфичних за окружења ИКС. Ове политике дефинишу најбоље праксе за обезбеђивање ИКС и пружају смернице које запослени и систем администратори треба да прате.
- ***Сарадња и размена информација***: Међу заинтересованим странама, укључујући владине агенције, индустријске организације и истраживаче. Размена информација о новим претњама, рањивостима и најбољим праксама може помоћи у побољшању укупне безбедности ИКС.

Иако су напади учесталији, примена добрих безбедносних мера је довела до тога да је у САД по истраживању [5] дошло до смањења пријављених успешних сајбер напада за 5.7 процената у години 2022 у односу на претходну, 2021 годину. Примери побољшања која су уведена на основу истраживања:

- ***Примена јаких полиса за аутентификацију*** – више факторска аутентификација, полиса која диктира комплексност шифре, полиса која ограничава време важења шифре, забрањено понављање шифре и брисање старих налога који се више не користе.
- ***Нису се поштовали стандарди*** – потребна су побољшања у областима управљања ризиком, управљања ризиком ланца снабдевања, управљања идентитетом и приступом, управљање конфигурацијом, заштите података и приватности, континуираног праћења безбедносних информација, реаговања на инциденте и планирања за ванредне ситуације.

2.2 Микросервисна архитектура

Архитектура микросервиса је позната више од једне деценије [22], али се још увек не користи у свим секторима. Заснована је на изградњи система као скупа више независних сервиса, од којих сваки ради као засебни процес, и који међусобно комуницирају. Главна предност у поређењу са традиционалним, монолитним архитектурама је то што се сервиси постављају одвојено. Још једна предност је вертикална скалабилност. Пошто се један чвор у микросервисној архитектури сматра одговорним за једну функцију, ако се повећа број захтева за ту функцију, могу се покренути више инстанци тог специфичног сервиса да одговори на повећано оптерећење. Предност разбијања монолита на више сервиса је већа толеранција на грешке. Ако једна функција монолита закаже, комплетан систем може постати неупотребљив. За микросервисе то није случај пошто су само погођене функције недоступне и ако не постоје зависности између њих, систем може наставити да пружа функције које су још увек доступне док се квар истражује и отклања.

Преглед тренутног стања безбедности у системима заснованим на микросервисима дат је у раду [33]. Аутори су анализирали 70 радова и сиву литературу (енг. *gray literature*) на ову тему и представили сумиране безбедносне идеје, принципе, анализе, механизме и дизајне који се користе за заштиту система заснованих на микросервисима. Декомпозицијом компоненти уводи се потреба за већим бројем комуникационих канала чиме се шири површина напада. Пошто су микросервиси дизајнирани да верују осталим микросервисина из кластера, компромитујући један, сви остали постају потенцијално експлоатисани.

У референци [34] аутори одговарају на питање „Који су ризици и како се они могу решити у раној фази или минимизирати након напада?“, дајући листу препорука. Као што је представљено у истраживању литературе [35], већина студија се фокусира на заустављање или ублажавање напада, а не много на опоравак од њих. Системи за детекцију упада могу се користити и у контејнерским окружењима [36]. Комуникација је највећа брига када је у питању обезбеђење архитектуре засноване на микросервисима, а испоставило се да су ауторизација и аутентификација најчешће коришћени безбедносни механизми [37]. Аутори су прегледом литературе открили да су протоколи OAuth 2.0 и OpenID Connect подобни за имплементирање аутентификације и ауторизације у микросервисним системима. Аутори референце [38] развили су оквир (енг. *framework*) за успостављање поверења и безбедну комуникацију. Тестирање је показало да су због комуникационих трошкова, перформансе система незначајно деградиране.

У раду [39] аутори предлажу водич за архитектуру и безбедност микросервисног система који је развијен коришћењем Spring Framework и Spring Security Framework. Доказали су да коришћење Spring Security Framework у комбинацији са OAuth2 протоколом може да обезбеди безбедност Spring-based API од Open Web Application Security Project Top 10 (OWASP) претњи. Критичне инфраструктуре често имају потребу да раде са великом количином података и често имају додирних тачака са IoT концептом. Занимљив приступ дефинисања безбедне IoT архитектуре је дат у раду [40] где је извршена анализа безбедносних захтева, изазова и претњи на основу чега је предложена нова безбедна архитектура. Аутори су дизајнирали и систем за верификацију безбедности којим се доказује да су сви безбедносни захтеви испуњени.

Резултат рада [41] је систематско мапирање претњи у микросервисним архитектурама и безбедносни предлози. Анализа је открила неравнотежу у истраживању

са нагласком на спољашње нападе и да су аудитинг и спровођење контроле приступа највише истраживане технике. Рад [42] истражује иновативне приступе заштити дистрибуираних услуга у микросервисној архитектури, с обзиром на проширену површину напада и изазове у централном логовању и отпорности на кварове.

Инсајдерске претње су присутне и у системима заснованим на микросервисима, посебно зато што је у примени микросервиса потребно укључивање специјалних алата за управљање. У референци [43] аутори идентификују претње интегритету и дефинишу скуп безбедносних захтева за системе засноване на микросервисима. Они предлажу оквир за заштиту интегритета који је отпоран на инсајдере.

Постоји више различитих опција када је у питању место инсталације односно поставке система који има микросервисну архитектуру [44, 45, 46]. Развој рачунарства у облаку доноси нове могућности када је поставка система (енг. *deployment*) у питању. Пружаоци услуга у облаку (енг. *cloud vendor*) као што су Google, Microsoft, Amazon и други нуде своје рачунарске ресурсе у закуп. Овим се терет одржавања рачунарских центара пребацује са компаније на пружаоца услуга у облаку. Облак је чест избор када је у питању развој и имплементација система који има микросервисну архитектуру [47]. У наставку су наведене неке предности ове везе:

1. ***Скалабилност и флексибилност***: Облак пружа ресурсе као што су виртуелне машине, складиште података, мрежну инфраструктуру на захтев. Једна од важнијих карактеристика микросервиса је скалабилност, што облак омогућава јер се нови ресурси могу брзо додати или уклонити у зависности од захтева.
2. ***Раздвајање функционалности***: Микросервисна архитектура подразумева раздвајање апликације на мање, независне сервисе који обављају специфичне функционалности. Облак омогућава повезивање и управљање овим сервисима, односно њихову ефикасну комуникацију.
3. ***Аутоматизација и оркестрација***: У облаку постоје алати за аутоматизацију и оркестрацију што је јако корисно за ефикасно управљање микросервисима. Контејнеризација (нпр. Docker) и оркестрациони системи (нпр. Kubernetes) се често користе како би се олакшало размештање, управљање и скалирање микросервиса.
4. ***Приступ ресурсима на даљину***: Микросервисима у облаку може се лако приступити са било ког места путем интернета. Овим се омогућава дистрибуирање тимова и глобално размештање апликација.

Инсталација система као што је ИКС у рачунарском облаку је примамљива због свих предности које облак доноси, али постоји и велика забринутост у вези са безбедношћу. Иако је важно заштитити систем на периметрима, што је углавном присутно и у традиционалним монолитним ИКС решењима, разбијање монолита на више микросервиса потенцијално уводи нове рањивости. Један пример решења безбедности као услуге представљен је у референци [48] у којој су аутори представили флексибилну инфраструктуру за праћење и спровођење полисе за мрежни саобраћај. Апликације у рачунарском облаку могу искористити ово решење за откривање и блокирање спољних и унутрашњих претњи. Иако је пребацивање одговорности на друге примамљиво, принцип нултог поверења постаје све популарнији [49]. Као што сама реч каже, овај принцип се заснива на третирању целокупног мрежног саобраћаја као непријатељског, при чему није важно да ли долази изнутра или изван периметра система. Имплементација нултог поверења између микросервиса може смањити ризик од извођења напада јер је потребно да сви корисници или чворови у систему буду аутентификовани и континуирано

валидирани док користе функције система. То је такође добра пракса када је у питању заштита система од инсајдера [29, 50, 51].

Имплементација Kubernetes и Istio сервисне мреже олакшава увођење нултог поверења у контејнерском окружењу. Референца [52] предлаже додатни скуп алата чија употреба може заштитити податке који се преносе између микросервиса. Урађена је занимљива студија о утицају имплементације модела нултог поверења на перформансе система [53]. Резултати су показали да је Istio смањио варијабилност латенције у одговору на секвенцијалне HTTP захтеве и да употреба процесора и меморије може бити повећана. Још један рад о заштити безбедносних података је [54] где су аутори применили нове полисе у моделу нултог поверења. Уводи се прокси за контролу приступа чији је задатак да анализира захтев за приступ, тип корисника, тип уређаја, тип апликације и тип података. Укупна стратегија за успостављање модела нултог поверења у окружењу рачунарства у облаку дата је у [55]. Пошто се окружењу у облаку не може веровати због његове динамичке и дељиве природе, главни изазов је заштита од крађе података. Аутори предлажу имплементацију механизма поверења, који ће динамички израчунавати поверење које се касније користи у захтевима за трансакције. Иако су користи од примене нултог поверења добро истражене, истраживање недостатака и трошкова нултог поверења је занемарено [56]. Изазови микросервисне архитектуре из погледа безбедности су описани детаљно у додатку Б.

2.3 Безбедна архитектура

У дизајн фази пројекта се анализирају како функционални тако и нефункционални захтеви на основу којих се израђује архитектура система. Врло је важно урадити добру анализу захтева јер неодговарајућа архитектура може у будућности да створи разне проблеме, као на пример проблем са перформансама, безбедности, додавање нових компоненти, функционалности и слично [20, 57]. Свака значајна измена архитектуре у фази имплементације или након пуштања система у рад је скупа. Један битан скуп нефункционалних захтева чине захтеви о безбедности система. Кључне безбедносне основе су наведене у додатку А. Ниво безбедности зависи од критичности система и често организације имају посебне тимове инжењера који се баве дефинисањем ових захтева. У случају критичних инфраструктура је безбедност јако битна јер ови системи морају да обезбеде функционалност и да буду доступни чак и током разних типова инцидената. Ако би дошло до неочекиваног престанка рада, настале би озбиљне последице по људске животе, животну средину или имовину.

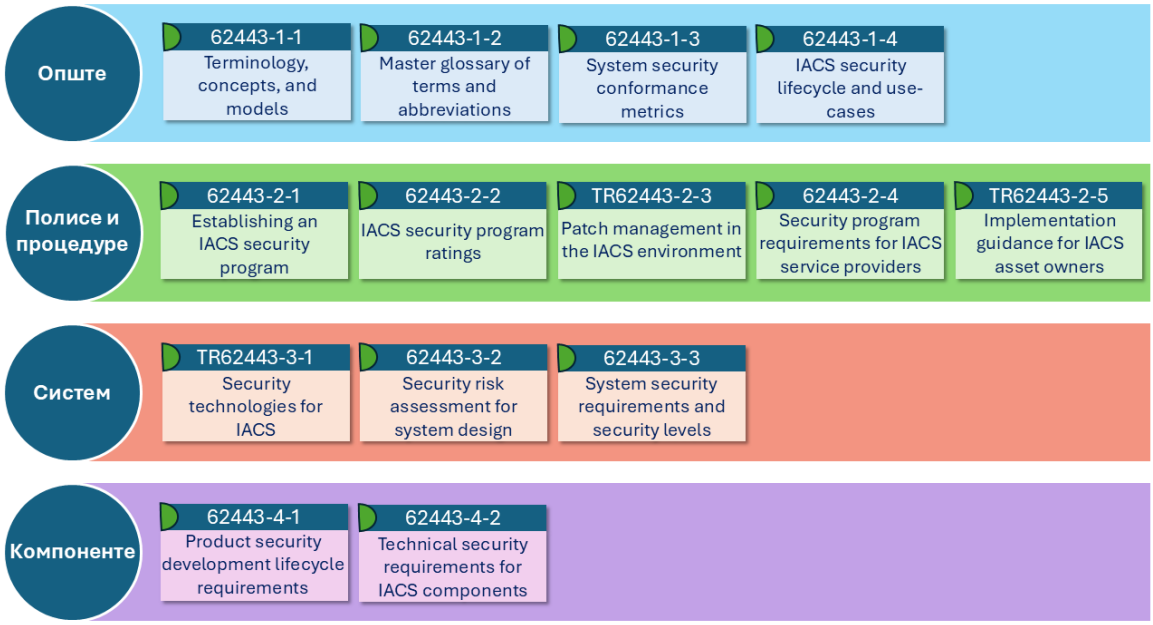
Циљ безбедне архитектуре је минимизовање ризика и одржавање континуиране функционалности система у екстремним околностима. Питање безбедности критичних инфраструктура је потребно истраживати из перспективе системског инжењерства. Безбедност треба да буде уграђена у архитектуру система на систематичан начин преко спектра свих компоненти, укључујући мрежу, контролни систем и процесе [8].

2.3.1 Стандарди

Примена стандарда осигурава да су системи дизајнирани поштујући најбоље праксе у индустрији, што смањује рањивост на сајбер нападе и друге ризике [20, 58]. Стандарди помажу у успостављању робусних процедура за одговор на инциденте и опоравак система након отказа. Регулисани сектори су суочени са законодавним захтевима који налажу примену одређених стандарда. Усаглашеност са стандардима

помаже организацијама да избегну правне последице и новчане казне, показује да организација озбиљно схвата безбедност и квалитет, што повећава поверење клијената, партнера и других заинтересованих страна. Представљају заједнички језик између различитих сектора и регулаторних оквира па као такви омогућују организацијама да лакше послују са међународним партнерима и клијентима. Мана стандарда је што се споро мењају и адаптирају на нове технологије, тако да компаније често излазе из њихових оквира како би остале конкурентне на тржишту. За International Organization for Standardization (ISO) прође генерално 5 године од тренутка дефинисања неке смернице док се она не усвоји као стандард [59]. Када је у питању безбедна архитектура ИКС следећи стандарди се издвајају:

1. **IEC 62443** серија стандарда дефинише захтеве за развој безбедних система за аутоматизацију и управљање (енг. *Industrial automation and control systems*, IACS) [60]. Обухвата све аспекте безбедности и покрива читав животни циклус система, од пројектовања до одржавања и праћења безбедности. Укупно има 14 стандарда који су подељени у четири целине где свака целина има другачији циљ (слика 2).



Слика 2 – ISA/IEC 62443 серија стандарда [60]

2. **ISO серија стандарда** [61]. **ISO/IEC 27001** је глобално прихваћен као водећи за управљање информационом безбедношћу. Осигурава да организације имају јак оквир за управљање, имплементацију, одржавање и побољшавање система за безбедност, укључујући управљање ризицима, контролу приступа и заштиту података [62]. **ISO/IEC 27017** проширује ISO/IEC 27001 и пружа додатне смернице специфичне за безбедност у окружењима у облаку. Укључује најбоље праксе за безбедну конфигурацију окружења у облаку, управљање подацима, контролу приступа и заштиту информација од неовлашћеног приступа и губитка информација. Јасно дефинише одговорности и обавезе између пружалаца услуга у облаку и њихових корисника, што помаже у избегавању конфликата и неодређености у погледу безбедносних мера. Обухвата и специфичне смернице за процену ризика у окружењима у облаку [63]. **ISO/IEC 27018** успоставља контроле и смернице за примену мера за заштиту личних података (Personally Identifiable Information – PII) у

складу са принципима приватности наведеним у стандарду ISO/IEC 29100 за јавни облак. Поред тога, документ наводи смернице на основу стандарда ISO/IEC 27002, узимајући у обзир регулаторне захтеве за заштиту личних података који могу бити примељиви у контексту окружења за управљање ризиком у вези са безбедношћу информација код пружаоца услуга јавног облака [64].

3. **NERC CIP** покрива широк спектар безбедносних мера и процедура које су неопходне за осигурање поузданости и безбедности електроенергетског система. Придржавање ових стандарда је обавезно за све ентитете који управљају критичном електроенергетском инфраструктуром у Северној Америци. NERC CIP стандард захтева идентификацију и примену одговарајуће заштите свих делова критичне инфраструктуре. Примена строгих контрола приступа је обавезна како би се повећала безбедност критичних инфраструктура. Ово укључује како физичку безбедност, тако и заштиту од сајбер претњи. Ови стандарди дефинишу и процедуре за континуирани надзор система, откривање и реаговање на безбедносне инциденте, као и извештавање о таквим инцидентима. Стандарди захтевају редовну обуку особља које ради на критичним системима, како би били свесни безбедносних ризика и знали како да реагују у случају инцидента [65]. **NERC CIP in the Cloud** се односи на примену критичних безбедносних стандарда за заштиту електроенергетских система када се инфраструктура и подаци премештају или управљају у рачунарском облаку. Овај приступ осигурава да се и у облаку поштују строге безбедносне смернице, као што су контрола приступа, надзор, и заштита података, како би се одржала поузданост и безбедност критичне електроенергетске инфраструктуре [66].
4. **SOC 2** стандард за ревизију и извештавање дефинише критеријуме за управљање осетљивим подацима клијената на основу пет кључних принципа (енг. *trust service principles*): безбедност, доступност, интегритет обраде, поверљивост и приватност (слика 3). SOC 2 је посебно важан за компаније које управљају подацима у облаку, јер осигурава да су њихови системи и процеси дизајнирани да заштите податке од неовлашћеног приступа и других сајбер ризика. Организације које успешно пролазе ревизију у складу са SOC 2 стандардом показују да испуњавају високе стандарде безбедности и управљања подацима, што може повећати поверење клијената и партнера [67].

Слика 3 – SOC 2 кључни принципи [68]

2.3.2 Смернице

За разлику од стандарда који дефинишу конкретне захтеве и критеријуме који морају бити испуњени и који су усвојени од стране признатих тела или организација, смернице су препоруке и савети који пружају упутства о томе како треба поступати у одређеним ситуацијама или како примењивати одређене процедуре и праксе. Оне нису обавезујуће и обично су флексибилније, омогућавајући организацијама да их прилагоде својим специфичним потребама и околностима [59]. Неке од смерница за ИКС су:

1. **NIST Cyber Security Framework v2** се фокусира на различите фазе управљања ризиком: идентификација, заштита, откривање, одговор, опоравак и управљање које су приказане на слици 4. По овом оквиру, безбедном архитектуром се успостављају мере контроле како би се смањила вероватноћа експлоатације претњи и напада на систем. У случају да се, упркос овим контролама, догоде напади, важно је открити их што пре и обезбедити одговарајуће механизме како би се ограничила штета што је следећа фаза. Мора се планирати и имплементирати одговарајући одговор. Коначно, након ове фазе, ако је дошло до штете, мора се обезбедити опоравак и обнављање система, а након тога и побољшање његове безбедности [69].

Слика 4 - Фазе управљања ризиком по NIST Cyber Security Framework v2 [69]

2. **NIST SP 800-53** "Security and Privacy Controls for Information Systems and Organizations" пружа свеобухватне смернице за управљање безбедносним контролама и приватности у информационим системима [70].
3. **NIST SP 800-190** "Application Container Security Guide" пружа смернице за безбедност контејнеризованих апликација, што је посебно важно за микросервисну архитектуру. Контејнери су често основа за микросервисе у окружењима у облаку, а овај стандард описује како да се обезбеде контејнери и управља ризицима у оваквом окружењу. Документ покрива аспекте као што су дизајн безбедне архитектуре, изолација, управљање тајнама и заштита података у контејнерским и микросервисним окружењима [71].
4. **NIST SP 800-82 Rev. 3** "Guide to Operational Technology (OT) Security" пружа преглед OT система, укључујући ИКС, идентификује уобичајене претње и рањивости над овим системима и даје препоручене мере безбедности за митигацију повезаних ризика [72].
5. **NIST SP 500-292** "NIST Cloud Computing Reference Architecture" дефинише референтну архитектуру облачног рачунарства. Даје детаљан приказ компоненти и актера у окружењу рачунарског облака, укључујући кориснике, пружаоце услуга и регулаторе. Такође помаже организацијама да боље разумеју како да користе облак на сигуран и ефикасан начин [73].
6. **NIST SP 800-144** "Guidelines on Security and Privacy in Public Cloud Computing" даје смернице за организације које користе јавни рачунарски облак, са фокусом на безбедност и приватност. У њему се објашњавају рањивости које су повезане са јавним рачунарским облаком, као и начини за њихово ублажавање. Обухвата теме попут контроле приступа, енкриптовања података, приватности корисника и правне обавезе коришћења облачних услуга [74].

7. **NIST SP 800-145** "The NIST Definition of Cloud Computing" пружа службену NIST дефиницију облачног рачунарства, која укључује кључне карактеристике, моделе имплементације и моделе услуга. У овом документу је описано пет основних карактеристика рачунарског облака, три модела услуга (IaaS, PaaS, SaaS) и четири модела имплементације (јавни, приватни, заједнички и хибридни облак) [75].
8. **ENISA Guidelines** је развијена од стране Европске агенције за сајбер безбедност и пружа смернице за различите аспекте сајбер безбедности, укључујући заштиту критичне инфраструктуре, управљање инцидентима, безбедност мреже и информационих система, као и заштиту података у окружењима у облаку. Помаже организацијама у усаглашавању са регулаторним оквирима Европске уније, као што су GDPR и NIS 2 директива. Смернице су прилагођене одређеним секторима па тако постоји одељак посвећен критичним инфраструктурама [76]. Смернице укључују и методологије за процену сајбер ризика као и препоруке за импелементацију мера за смањење ризика. Помаже едукацији корисника пружајући алате и ресурсе за обуку.
9. **OWASP Cloud-Native Application Security Top 10** листа има за циљ да пружи смернице за безбедност апликација у окружењима у облаку, укључујући препоруке за архитектуру и најбоље праксе за заштиту [77]. Бави се следећим кључним тачкама: конфигурација инфраструктуре, управљање тајнама и осетљивим подацима, обезбеђење интерфејса, управљање привилегијама, заштита од сајбер напада.
10. **SANS TOP 25** листа најчешћих софтверских грешака и рањивости које могу довести до озбиљних безбедносних проблема у апликацијама. Ова листа је развијена у сарадњи између SANS Института, MITRE и других експерата за сајбер безбедност. Садржи и рангирање према озбиљности, учесталости појављивања и утицају као и препоруке за ублажавање [78].
11. **CSA Cloud Controls Matrix (CCM)** је свеобухватни оквир за безбедносне контроле фокусиран на окружења у рачунарском облаку. Састоји се од 197 контролних тачака које су подељене у 17 домена [79]. Дизајниран је да буде компатибилан и усклађен са другим глобалним стандардима и регулативама, као што су ISO/IEC 27001, NIST SP 800-53, GDPR, и други. Његовим коришћењем организације могу да процене ефикасност постојећих контрола и да идентификују области које захтевају додатну пажњу. Пружаоци услуга у облаку углавном јавно објаве своју листу као што је приказано у [80] за AWS.
12. **Center for Internet Security benchmark** је скуп најбољих пракси и смерница за конфигурацију различитих типова система, укључујући и системе у облаку [81]. Имају редовна ажурирања тако да су увек у складу са најновијим претњама и технологијама и тако помажу организацијама да побољшају своју сајбер безбедност и смање ризике од сајбер напада.

2.3.3 Законски оквир

Законски оквир (регулатива) чине званични закони, правила или прописи које доносе владини органи или надлежне институције са циљем да регулишу одређене активности, понашања или процесе у друштву. Непоштовање регулатива може довести до правних последица, као што су новчане казне, санкције или друга правна одговорност. Постављају оквире и услове под којима се одређене активности могу обављати, са циљем заштите јавног интереса, безбедности, здравља, приватности или других важних аспеката друштва.

1. **General Data Protection Regulation (GDPR)** регулатива ЕУ поставља строге захтеве за заштиту података и приватност грађана ЕУ. Применљива је на све оганизације које обрађују личне податке грађана ЕУ и има глобални домет. Када су у питању права везана за личне податке, грађани имају права на приступ, исправку, заборав и пренос података. Прописане су основе и мере за заштиту података које организације морају имплементирати. Поред тога, организације морају имати сагласност од појединца пре него што крену да обрађују његове податке [82].

2. **NIS 2 direktiva** – ажурирани правни оквир ЕУ који поставља захтеве за обезбеђење мрежних и информационих система унутар држава чланица ЕУ. Ова директива је наставак и проширење оригиналне NIS директиве, која је била први свеобухватни закон ЕУ усмерен на повећање сајбер безбедности широм ЕУ [3]. Обухвата већи број сектора и врста организација. Директива поставља строже захтеве за управљање сајбер ризицима и спровођење мера за спречавање сајбер инцидената, као и мера за брзо и ефикасно реаговање у случају инцидента. Захтева већу координацију и размену информација између држава чланица ЕУ и различитих актера на пољу сајбер безбедности. Организације које су обухваћене NIS 2 директивом морају пријавити значајне сајбер инциденте надлежним органима власти у кратком временском року, како би се омогућила брза реакција и минимизирали потенцијални штетни утицаји.

2.3.4 Захтеви

Што се тиче три основна захтева за безбедност, поверљивост, интегритет и доступност (енг. *Confidentiality, Integrity, and Availability*, CIA), ИКС често захтева да његова доступност буде приоритетна у односу на интегритет и поверљивост [83, 84, 85]. Претња над доступности би учинила основне контролне, перформансе и информативне ресурсе недоступнима, претња над интегритетом се одражава као манипулација критичним хардвером, софтвером или подацима, док искоришћење претње над поверљивости значи прислушкивање осетљивих информација. Модел за безбедност ИКС може бити разрађен да успостави неколико фундаменталних захтева, укључујући контролу приступа, контролу коришћења, интегритет података, поверљивост података, ограничен ток података, правовремени одговор на догађаје и доступност ресурса. У табели 2 је дат приказ највероватнијих претњи над ОТ системом на основу тога који елемент CIA тријаде би био највише погођен ако се те претње остваре [86].

Табела 2 – Груписање претњи ИКС паметних мрежа на основу ЦИА тријаде

CIA	Претња
Поверљивост	Губитак поверљивости конфигурационих података
	Губитак поверљивости оперативних података
Интегритет	Неовлашћена измена или брисање конфигурационих података
	Неовлашћена измена или брисање оперативних података
Доступност	Напад ускраћивања услуге (енг. *Denial of Service,* DoS) на позадинске сервисе
	Испад позадинских сервиса због лоших података
	DoS напад на комуникационе канале, нпр. мобилне или мрежне комуникације недоступне услед напада
	DoS напад на интерфејс човек-машина

Шири скуп безбедносних захтева над ИКС је приказан у додатку Д. Стандард IEC 62443 прописује следећих седам основних захтева:

1. Контрола идентификације и аутентификације (енг. *identification and authentication control*) корисника, процеса и опреме пре него што им се дозволи приступ

2. Контрола употребе (енг. *use control*) осигурава да сви идентификовани корисници (људи, процеси и опрема) имају привилегије за извођење потребних радњи у систему и праћење активности корисника, односно употребу тих привилегија

3. Интегритет система (енг. *system integrity*) тј. заштита од неовлашћених промена комуникационих канала и складишта података

4. Поверљивост података (енг. *data confidentiality*) је способност спречавања цурења информација у комуникационим каналима и складиштима података

5. Ограничење протока података (енг. *restrict data flow*) карактерише ниво сегментације система на зоне и канале како би се избегло непотребно ширење података

6. Време одзива система на догађај (енг. *time response to an event*) мери ниво оперативног надзора ИКС и способност реаговања на инциденте у предвиђеном року

7. Доступност ресурса (енг. *resource availability*) мери ниво заштите како би се осигурала доступност система од напада ускраћивања услуга, способност рада у деградираном режиму и способност опоравка од њих

2.3.5 Тестирање безбедности

Процес тестирања безбедности система обухвата низ корака и метода које се користе како би се проценила ефикасност заштите система од потенцијалних претњи и коришћења рањивости. Први начин је **анализа рањивости** (енг. *vulnerability analysis*) што представља системску анализу архитектуре како би се идентификовале познате и потенцијалне рањивости. Откривањем рањивости могу се предузети кораци за њихово отклањање. Следеће је **пенетрационо тестирање** (енг. *penetration testing*) где се ангажују безбедносни стручњаци који покушавају да провале у систем искоришћавањем његових рањивости. Циљ је идентификовање слабости и откривање како нападач може да их искористи. Врло је корисно спроводити **симулације разних напада** што даје увид у то како систем реагује на различите сценарије напада. Уз то се и тестира реакција система на стварне претње. **Анализа изворног кода и архитектуре** је важан јер помаже у откривању потенцијалних рањивости, односно лоших пракси у дизајну. **Тестирање перформанси под оптерећењем** помаже у утврђивању како се систем понаша у екстремним ситуацијама, укључујући и инциденте. **Коришћење безбедносних стандарда** и смерница као основу за процену безбедности, на пример анализа архитектуре система у односу на релевантне стандарде и смернице као што су ISO 27001, NIST, OWASP. **Спровођење редовних безбедносних ревизија** може помоћи у процени нивоа безбедности система и идентификацији области које захтевају побољшања. Тестирање безбедности система треба да буде континуиран процес јер се претње и рањивости могу мењати током времена.

Пример процене безбедности ИКС је дат у раду [87] у ком аутори предлажу следеће фазе:

1. Анализа ИКС, идентификовање и прикупљање информација о компонентама из којих се систем састоји које су битне са становишта безбедности. Битни елементи су сервиси и токови података.
2. Реконструкција ИКС у симулационом окружењу. Спровођење експеримената над системом у продукцији је ризично и из тог разлога је потребно креирати што реалнију реплику система која ће да се користи у сврхе тестирања.
3. Идентификација сценарија употребе са фокусом на прикупљање информација о корисницима, правима приступа, безбедносним полисама.
4. Дизајн експеримената дефинише циљеве напада и који делови система ће бити афектовани. Након тога се описује сценарији за напад као и кораци који су потребни за успешно извршен напад.
5. Извршавање аутоматизованих екперимената осигурава да ће сваки експеримент бити идентичан. Ово је важно јер тако може да се прати прогрес у развоју безбедности система.
6. Прихват и анализа резултата током трајања експеримента омогућава долазак до закључка о стању безбедности система. Тамо где су откривене рањивости система се препоручују мере за митигацију.

Постоје разни софтвери који служе као симулатори напада. Један такав софтвер је приказан у раду [88]. MAlSim – Mobile Agent Malware Simulator може да симулира различитих фамилија малвера (црви, вируси, малициозан код, итд.) као и различите врсте унутар исте фамилије. Поред симулације малвера, може да симулира генеричко понашање као што је слање фајлова или порука и непостојећу конфигурацију.

3. АНАЛИЗА БЕЗБЕДНОСТИ ИКС

Већина метода за анализу ризика ИКС прати ISO 27005 и стога имају заједничке тачке [89] које обично укључују анализу компоненти система, идентификацију ризика на основу генеричких листа и њихову процену коришћењем добро дефинисане скале. На слици 5 је представљен генерални приступ анализе ризика:

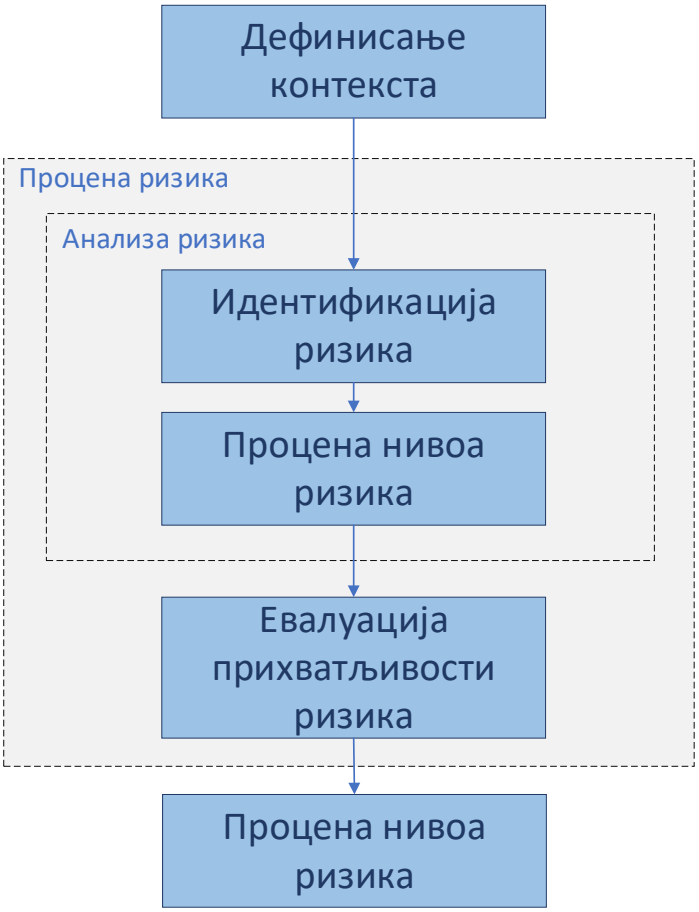
1. Дефинисање контекста обухвата кораке пописивања елемената система, идентификовања свих хардверских и софтверских компоненти. Поред тога, обухвата и дефинисање метрика за вероватноћу, утицај и ниво ризика и рањивости.

2. Идентификација ризика идентификује узроке који би могли довести до нежељених догађаја, односно потенцијалне рањивости или слабости различитих елемената система.

3. Процена нивоа ризика на основу вероватноће и утицаја коришћењем матрице ризика.

4. Евалуација прихватљивости ризика

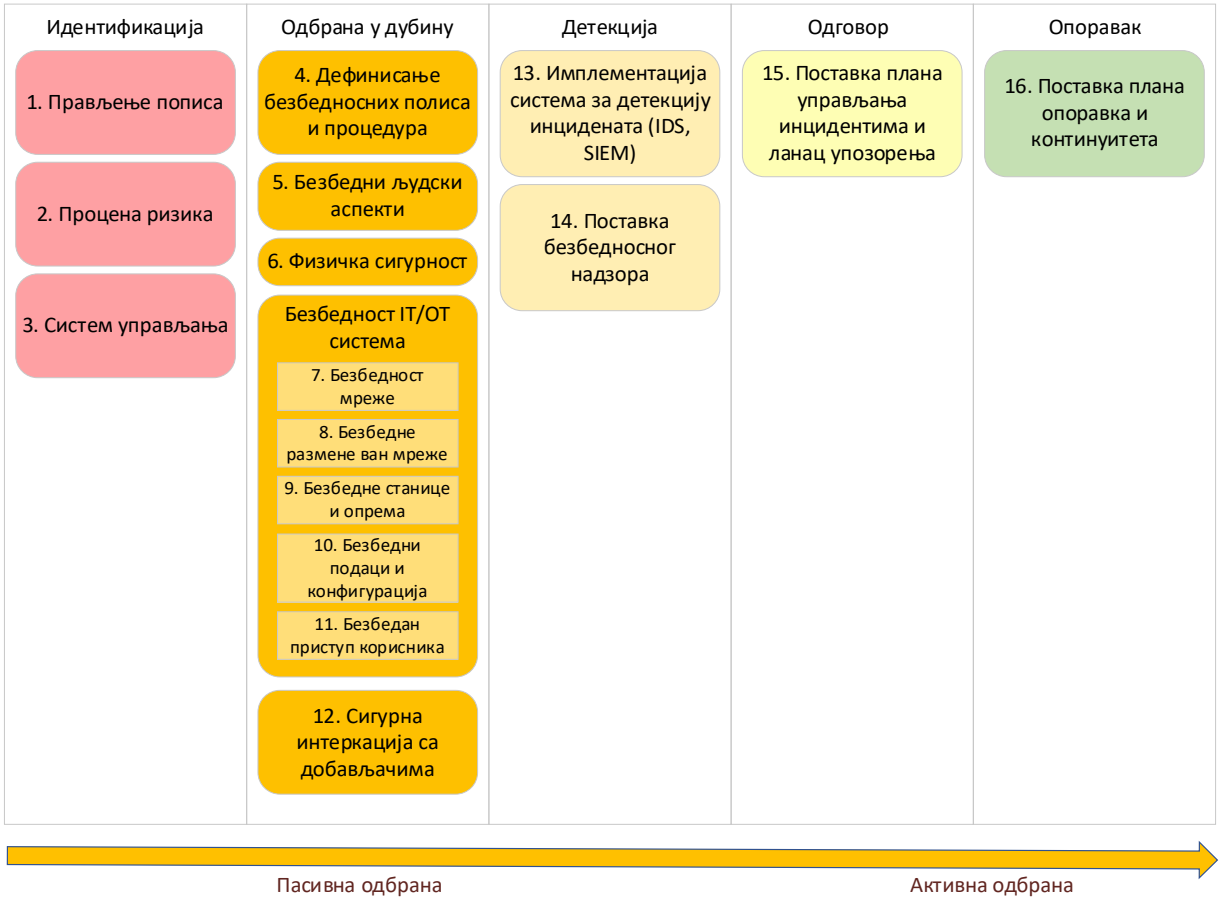
5. Третирање ризика преко дефинисања мера које је потребно предузети да би се ризик елиминисао или смањио.



Слика 5 – Генерални приступ анализи ризика [89]

3.1 Кораци анализе ризика

Детаљнији кораци су представљени на слици 6 вођени препорукама NIST оквира [89]. Кораци се могу класификовати у пет категорија: идентификација, одбрана у дубину, детекција, одговор, опоравак. За сваки корак су наведене мере које безбедни ИКС треба да испуне.



Слика 6 – Кораци у безбедности ИКС [89]

3.1.1 Идентификација

1) Попис елемената система (хардверске, софтверске компоненте и комуникациона опрема) и њихових интеракција са физичким окружењем. Анализа референтног ОТ система који је коришћен у овој дисертацији је презентована у овом поглављу.

2) Процена нивоа ризика, какви су утицаји сајбер напада у контексту последица на људе, имовину или производне капацитете. Поред утицаја, потребно је анализирати и вероватноћу, узимајући у обзир рањивости ИКС и предузете мере безбедности.

3) Поставити систем управљања у ИКС који јасно дефинише шта је чија одговорност и задатак. Ово је битно да би управљање безбедношћу ИТ и ОТ система била униформна.

3.1.2 Заштита

4) Дефинисати полисе и процедуре. Улоге и одговорности свих учесника јасно дефинисати, посебно између ИТ и ОТ подсистема и спољашњих учесника. Поред тога, дефинисати и правила за: управљање корисничким налозима, коришћење преносних медија, удаљени приступ, коришћење мобилних уређаја, коришћење

личних рачунара, управљање антивирусом, управљање безбедносним ажурирањима, управљање променама, процедуре за прављење резервних копија и опоравак, и одговор на инциденте.

5) Одговарајућа периодична едукација о безбедности и психолошке провере су од суштинског значаја за све запослене. Тренинзи су прилагођени радном месту. Тако постоје тренинзи за операторе, менаџере, запослене који се баве одржавањем или развојем, новозапослене, екстерне сараднике и за посетиоце.

6) Физичка сигурност опреме се осигурава инсталацијом видео надзора, аларма, ограда, ангажовањем чувара и слично. Операторске радне станице морају бити у физички изолованој просторији која се стално надгледа и приступ овој просторији треба да имају само запослени са одговарајућим привилегијама.

7) Осигурати безбедност мреже. Постојећа мера је коришћење препоручених индустријских протокола за комуникацију са уређајима у пољу. Комуникациони канал су кодирани и постоји мрежна баријера на периметрима система који филтрира долазни и одлазни саобраћај.

8) Заштита размене ван мреже. Преносни медији као што су USB или чврсти диск не смеју да се користе. Трансфери потребних података се обављају користећи радну станицу која је намењена за те врсте активности и која има инсталиран антивирусни програм.

9) Заштита радних станица и сервера подразумева следеће добре праксе: деактивација подразумеваних налога, затварање портова који се не користе, деинсталација непотребних апликација (на пример алата за тестирање и откривање грешака), редовно постављање безбедносних закрпа, увођење листе дозвољених апликација. Поред физичке сигурности PLC и осталих уређаја у пољу потребно је заштитити приступ лозинком, искључити удаљени приступ уколико је то могуће. Ограничити комуникацију само на дефинисане IP адресе. Редовно се ажурира фирмер (енг. *firmware*) и мења лозинка.

10) Гарантовати безбедност података и конфигурације. Интегритет података се обезбеђује кроз енкрипцију саобраћаја и безбедних складишта података. Сви битни подаци, као што је на пример инсталација су потписани сертификатом како би се утврдила њихова аутентичност. Бинарне датотеке које садрже осетљиве информације морају да буду замагљене (енг. *obfuscated*).

11) Приступом корисника се управља на основу улога, имплементирајући принцип нижих привилегија (енг. *least privilege*) и раздвајање дужности (енг. *separation of duties*). Постоји процес за креирање, управљање, верификовање, поништавање и ревидирање идентитета корисника који морају бити аутентификовани и ауторизовани како би користили функције система.

12) Обезбеђивања интеракције са добављачима и пружаоцима услуга. Најбоље је бирати сараднике који имају неки од признатих сертификата.

3.1.3 Детекција

13) Систем за откривање инцидената. Сви релевантни елементи система бележе догађаје који се даље обрађују и од њих се креирају аларми.

14) Надзор безбедности. Додавање или измена компоненти система мора да буде испраћена и у документацији. Редовно праћење рањивости хардвера и софтвера осигурава да се у најкраћем року поставе најновије безбедносне закрпе. Редовни пенетрациони тестови како би се открили аномалије на време.

3.1.4 Одговор

15) Поред правовремене детекције инцидента, битно је имати дефинисано шта се ради када се инцидент десио, ко треба да добије обавештење у зависности од нивоа важности инцидента и које мере треба применити у фази одговора.

3.1.5 Опоравак

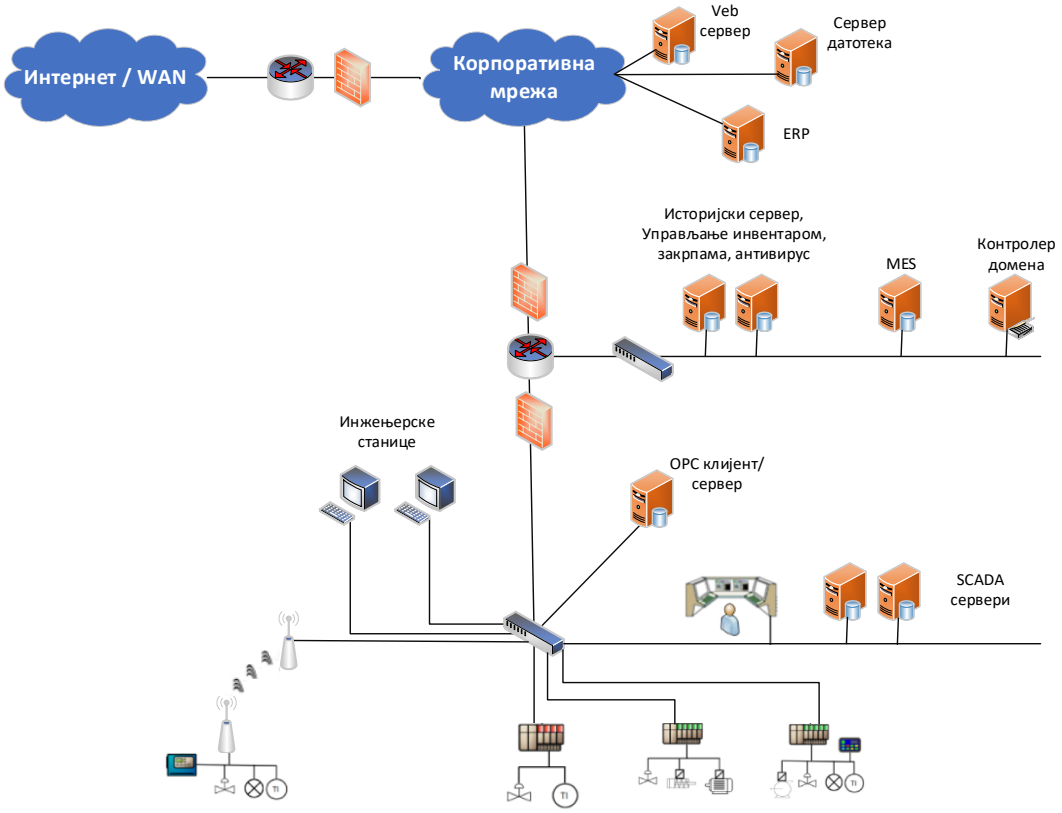
16) Битно је имати план за поновно оспособљавање система након инцидента. Потребно је имати јасно дефинисану политику за прављење периодичних резервних копија система, база података, PLC, конфигурација, контролних параметара. План континуитета пословања мора да постоји и он укључује постојање копије система на удаљеној локацији на коју могу да се преусмере корисници уколико дође до катастрофе.

3.2 Типична архитектура ИКС

Стандард IEC-62443 предлаже типичну архитектуру ИКС, приказану на слици 7. Угрубо, ИКС се деле на два подсистема и то су ИТ и ОТ. Главна разлика је у домену одговорности, ИТ подсистем управља подацима у оквиру пословног домена док је ОТ одговоран за управљање физичким процесима и уређајима у пољу [90]. Грануларнија подела је представљена у стандарду IEC-62443 и то су следећих 5 нивоа:

1. ***Процесно окружење*** – овај ниво садржи физичке системе који се користе у продукцији. Сензори и актуатори се налазе на овом нивоу као и удаљени RTU уређаји.
2. ***ОТ подсистем*** – укључује компоненте које служе за надзор и контролу физичких процеса, опреме и догађаја из контролног центра. ОТ подсистеми су кључни за функционисање индустријских операција јер обезбеђују директну интеракцију са физичким компонентама производних процеса. На пример, SCADA је део ОТ подистема.
3. ***ОТ DMZ*** – омогућава контролисан проток информација између ОТ и ИТ зона. У овој зони се налази база података и компонента чији задатак је да складишти историјске податке.
4. ***ИТ подсистем*** – садржи хардвер, софтвер и комуникационе технологије чији је фокус на складиштењу, опоравку, преносу, манипулацији и заштити података.

5. ***ИТ DMZ*** – зона која традиционално једина има приступ интернету и којој се једино може приступити са интернета. У овој зони се налазе веб сервери, сервери који служе за интеграцију са другим системима и слично.



Слика 7 - Типична ИКС архитектура [89]

3.3 Референтни систем

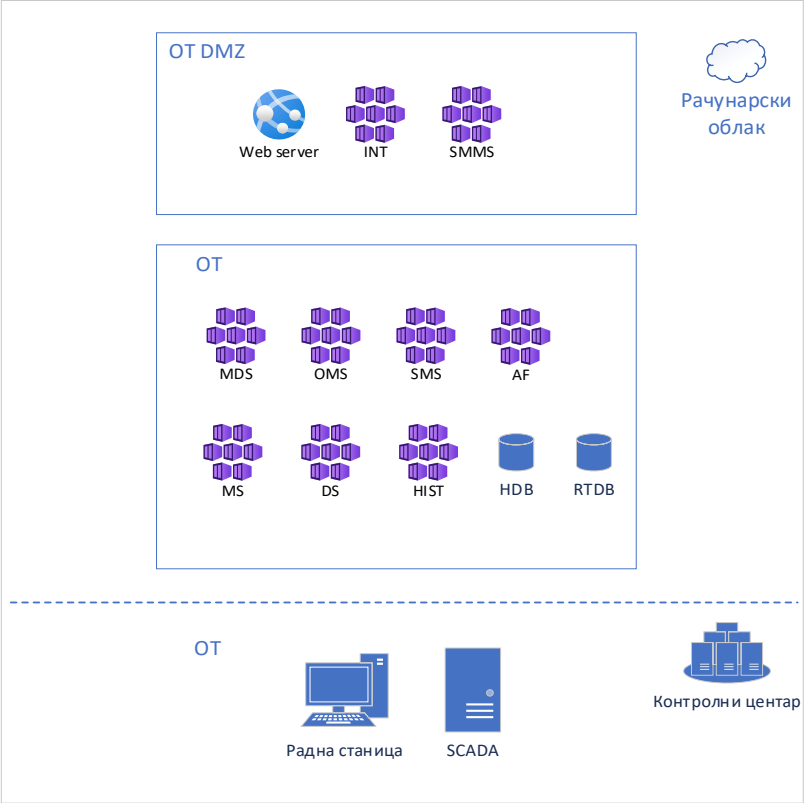
За потребе израде ове докторске дисертације, моделован је реалан систем који испуњава следеће критеријуме:

- Користи се у критичној инфраструктури,
- Има микросервисну архитектуру,
- Постављен је у рачунарски облак,
- Садржи сервисе различитих функционалности које немају исти ниво критичности.

У овом истраживању, фокус ће бити на ОТ подсистему чији је један део заснован на микросервисној архитектури и постављен у рачунарски облак. Примена ове архитектуре повећава скалабисност система [7] јер ако је потражња већа, број микросервисних инстанци се може повећати. Поставка система у рачунарски облак смањује потребне трошкове унапред и укупну потрошњу. Главни недостатак овог приступа је што се уводе нови безбедносни ризици јер је систем сада изложен јавном интернету и пружаоцу услуга у рачунарском облаку и у ОТ и ОТ DMZ зонама.

Моделовани систем приказан на слици 8 садржи десет сервиса и две базе података где је сваки сервис постављен као посебан микросервис у кластеру. Као приступне тачке

постоје још два сервиса који нису део кластера већ су део традиционалног ОТ подсистема који се налази на серверима који нису у рачунарском облаку. То су клијентска апликација која се користи за управљање системом и његовим функцијама и SCADA преко које систем добија статус опреме на пољу и извршава командовање том опремом. Уређаји у пољу не комуницирају само преко SCADA система већ могу и директно да шаљу своја мерења веб или SMMS сервисима на пример.



Слика 8 – Референтна ИКС микросервисне архитектура

Компоненте система се могу поделити у четири групе:

1. ***Периметарски сервиси*** – улазна тачка у систем је сервис за размену порука (енг. *Messaging Service*, MS) и његова одговорност је да преусмери клијентске захтеве на одговарајући сервис. Свака промена која долази из процесног окружења (SCADA) се обрађује у сервису динамике (енг. *Dynamics Service*, DS) и чува у бази података (енг. *Real-time Database*, RD). Комуникација је двосмерна, што значи да се статус удаљених тачака може мењати преко овог сервиса.

2. ***Основни сервиси*** – сервис за управљање статичким моделом (енг. *Model Service*, MDS) је одговоран за одржавање модела који ИКС користи и за координисање ажурирања модела. Сервис за управљање испадима (енг. *Outage Management Service*, OMS) бележи случајеве испада у пољу, дефинише планове опоравка и врши аутоматске радње за опоравак уколико је то могуће. Сервис задужен за вођење евиденције о поправкама и креирање радних налога за слање екипа на терен је сервис управљања поправкама (енг. *Switching Management Service*, SMS). Аналитичка функција (енг. *Analytics Function*, AF) је микросервис који служи за покретање одређених прорачуна који могу бити различити у зависности од типа ИКС. Сервис за

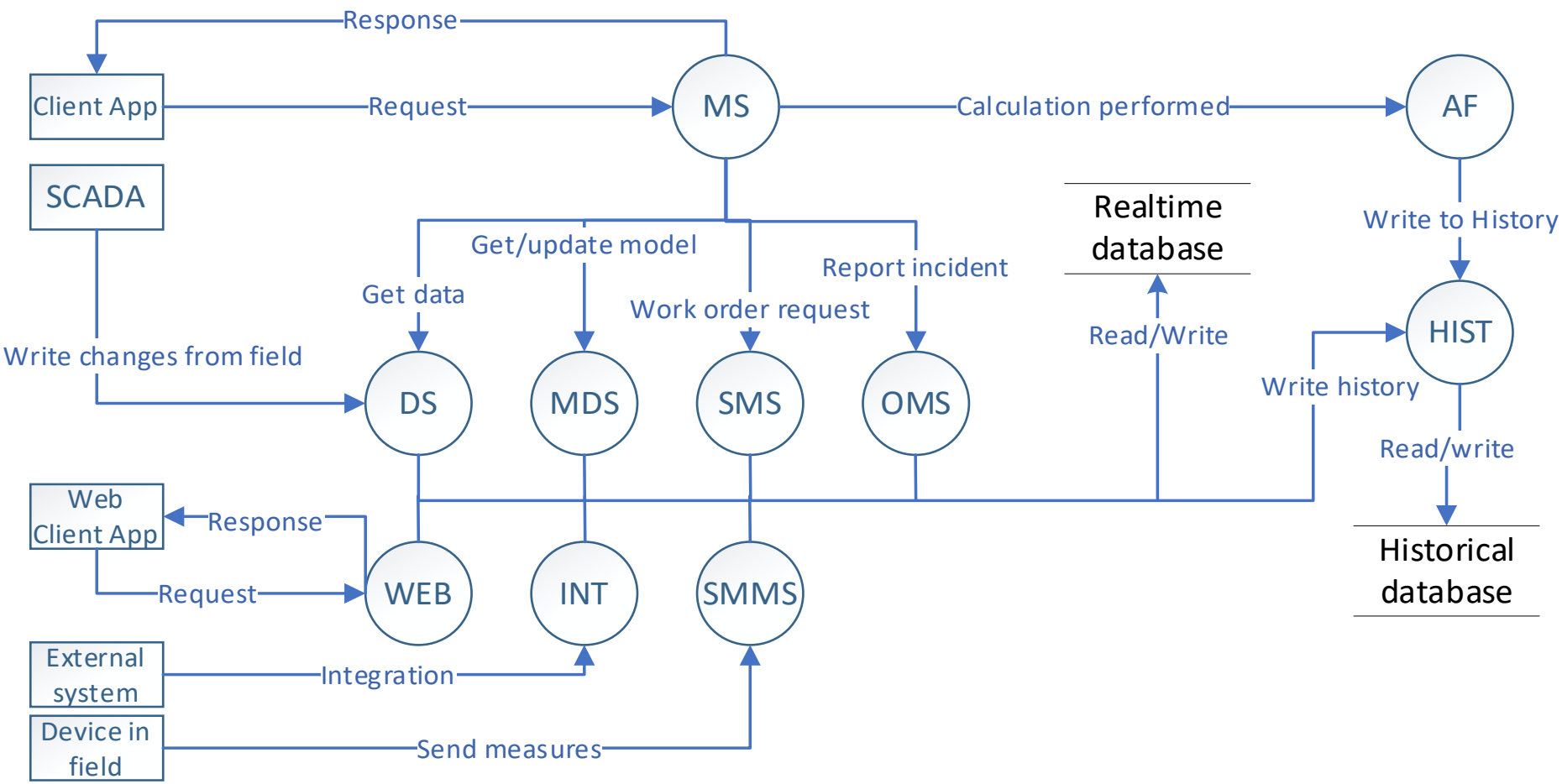
историју (енг. *Historical*, HIST) је компонента која се користи као приступ историјској бази података.

3. ***Јавни сервиси*** – ово су сервиси који су јавно доступни и којима се може приступити са интернета. Интеграциони сервис (енг. *Integration Service*, INT) омогућава повезаност са екстерним информационим системом који одржава други актер. На пример интеграција са провајдером времена. Прикупљање информација и комуникација са паметним бројилима се одвија преко сервиса за управљање паметним бројилима (енг. *Smart Meter Management Service*, SMMS). Приступ одређеном скупу функционалности је могућ и преко интернета и те функционалности су имплементиране у веб серверу и на тај начин омогућене крајњим корисницима.

4. ***Складиштење података*** – RD садржи информације о тренутном стању сензора и актуатора. Свака промена у систему се чува у историјској бази података (енг. *Historical Database*, HD).

3.4 Токови података референтног система

Поред анализе компоненти које су саставни део система, потребно је дефинисати и везе између њих, улазе, излазе и све могуће случајеве коришћења система. Ове информације су садржане у дијаграму токова података који је приказан на слици 9.



Слика 9 – Токови података

Сваки сервис дефинише листу метода, односно услуга које нуди другим микросервисима и екстерним апликацијама, уређајима који нису саставни део система и налазе се изван кластера микросервиса. Екстерне апликације су приказане на левој страни дијаграма и то су клијентска и веб апликација, SCADA, екстерни систем који се користи за интеграције и уређаји у пољу који директно комуницирају са микросервисима. Постоје следећи токови података:

- Клијент иницира различите акције, пристигле захтеве прво обрађује MS и онда их прослеђује одговарајућем сервису. На пример ажурирање или приказ модела, приказ стања опреме, приказ историје, прорачун који спроводи аналитичка функција и слично. У току обраде ових захтева сервиси приступају бази.

- Мањи скуп активности клијент може да извршава користећи веб клијентску апликацију. Ове захтеве обрађује веб сервер који комуницира са одговарајућим сервисом како би извршио тражену акцију.

- Клијент пријављује квар или инцидент користећи клијентску апликацију. MS захтев прослеђује OMS, који заводи инцидент у базу и креира план опоравка. Уколико план захтева неке ручне акције, OMS контактира SMS који издаје налоге за слање потребне екипе на терен. За аутоматске акције OMS шаље захтеве DS који их обрађује и даље прослеђује на SCADA.

- SCADA шаље промене из поља сервису динамике DS који те промене обрађује, освежава стање опреме у бази и бележи у историјску базу. Други смер је такође могућ, где корисник издаје команду за промену статуса опреме у пољу. Користећи клијентску апликацију, корисник шаље захтев ка систему који прво обрађује MS и даље прослеђује DS који даље издаје команду SCADA систему.

- Могућа је интеграција са екстерним системима. Ови системи се интегришу преко INT сервиса који даље комуницира са осталим сервиса у зависности која је интеграцију у питању. Пример екстерног система би био систем за аутоматску пријаву кварова или систем за временску прогнозу.

- Уређаји у пољу могу директно да комуницирају са системом преко SMMS. Статус ових уређаја SMMS уписује у базу и бележи у историју.

3.5 Анализа рањивости референтне архитектуре

Успешност напада у великој мери зависи од рањивости ИКС, односно сајбер претњи којима је изложен. Стога, истраживања о рањивостима ИКС помажу у разумевању осетљивих тачака за покретање злонамерних напада. Пре истраживања фокусираних, треба анализирати и генеричке рањивости које су присутне у сваком систему [84]:

- Инсајдерска претња од запослених, бивших запослених, консултаната, екстерних експерата. Злонамерни инсајдери, запослени који праве грешке и занемарују политике, инфилтратори који добију легитимни спољни приступ без одобрења.

- Злоупотреба недостатка процедура за пријављивање безбедносних слабости.

- Крађа корисничких кредeнцијала и њихова злоупотреба.
- Коришћење неадекватног помоћног софтвера.
- Злоупотреба критичних грешки у софтверу, нпр. прекорачење бафера (енг. *buffer overflow*).
- Неауторизовано брисање фајлова.
- Безбедносне претње проузроковане недовољним тестирањем приликом примене нових закрпа (енг. *patches*) или софтверске грешке након испорученог софтвера.
- Нарушавање поверљивости, доступности и интегритета конфигурационих података.
- Нарушавање поверљивости, доступности и интегритета записа.
- Нарушавање поверљивости, доступности и интегритета операционих података.
- Безбедносне претње проузроковане неисправношћу опреме, нпр. неисправна мерења сензора.
- Нарушавање поверљивости, доступности и интегритета личних података.
- Безбедносне претње проузроковане DoS/DDoS нападима на позадинске сервисе и комуникациону мрежу.
- Безбедносне претње настале услед прекида рада мреже.
- Безбедносне претње настале услед намерног оптерећења мреже манипулацијом потрошачких уређаја.
- DoS/DDoS напади на корисничке апликације.

Уопштено, ИКС не само што има подскуп рањивости наслеђен из IT домена, већ такође уводи и додатне рањивости јединствене за одређени ИКС. Рањивости могу постојати широм компоненти ИКС, као што су полиса управљања, системска архитектура, комуникационе мреже и уређаји на терену. Рањивости ИКС могу бити класификоване у пет главних категорија као што је резимирано у Табели 3.

Табела 3 – Главне категорије потенцијалних рањивости ИКС [31]

Категорија	**Рањивост**
Подаци	Одсуство или неадекватна идентификација и класификација података у ИКС.
Безбедносне процедуре и администрација	Неадекватно управљање безбедношћу у областима полиса и процедура
	Неефикасно управљање конфигурацијом због примене неформалних процедура
	Не постоји формална обука и свесност за безбедност ИКС
Мрежа	Рањивости комуникационог протокола, периметра и комуникационог канала
	Доступна је само основна провера интегритета података, а евидентирање и вођење записа углавном не постоје, што чини управљање конфигурацијом и форензику изузетно тешким
	Слепо поверење у способност ИКС веза да поуздано преносе податке и у повезивање ИКС са спољним мрежама
Архитектура	Коришћење ИКС комуникационих веза и мрежа за пренос сигнала повезаних са хитним службама као што су сигурносни и противпожарни системи, што повећава потенцијал за упаде и прекиде
Платформа	Рањивости хардвера и софтвера
	Недовољно заштићене лозинке за платформу или уређаје
	Даљински приступ и конфигурација доступни RTU уређајима који имају слабости у аутентификацији
	Постепени прелазак система на платформу рачунарства у облаку

Рањивости процедура често постоје због непотпуне, неодговарајуће или непостојеће безбедносне документације, као што су полисе и упутства за процедуре коришћења лозинки и одржавања система. Платформске и мрежне рањивости пре свега потичу од дизајна и развоја компоненти и система. Слабост у архитектури може изазвати утицај на безбедност целог система. На пример, ако је лични рачунар запосленог у корпоративној мрежи заражен вирусом због недостатка или неажурираног антивирусног софтвера, цео ИКС може бити погођен преко интернета. Рањивости у конфигурацији

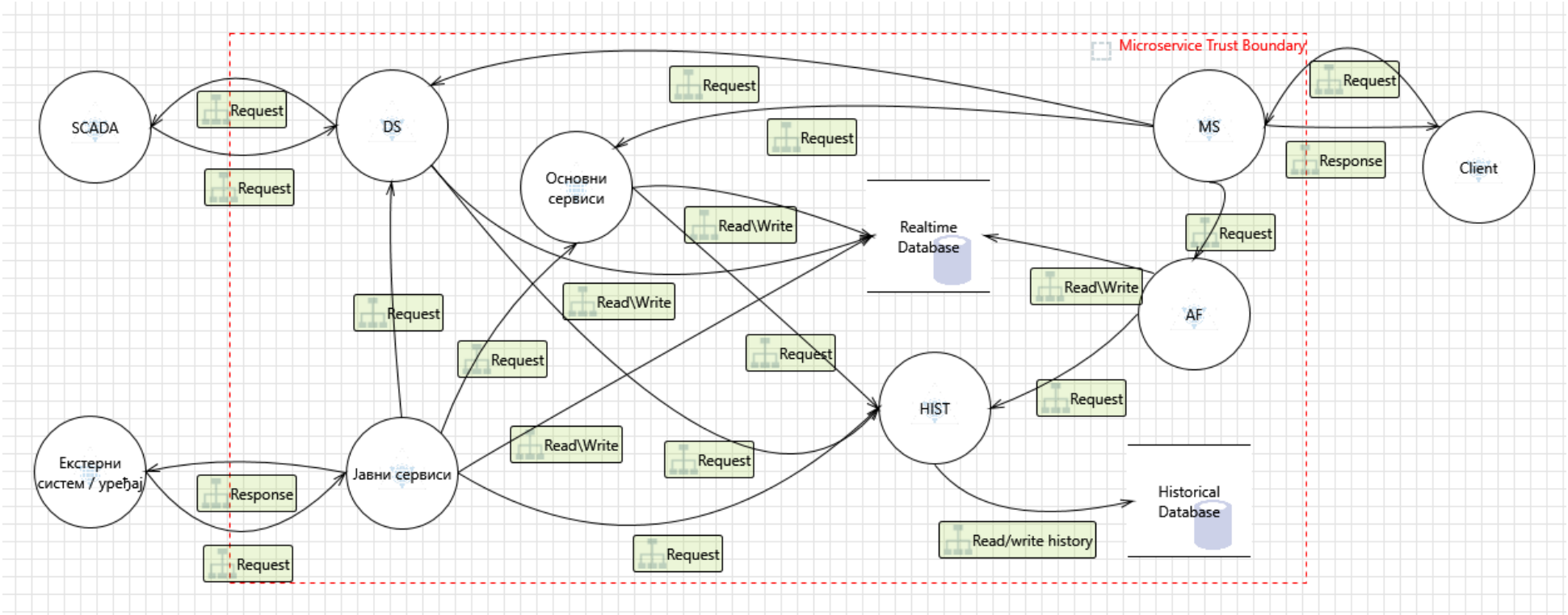
мреже (нпр. корпоративна мрежа не конфигурише правилно листе за контролу приступа или шаље лозинку у обичном тексту) такође могу узроковати нападе на систем. У наставку (табела 4) су наведене детаљније слабости, по слојевима ИКС [6].

Табела 4 – Рањивости по слојевима ИКС

Слој система	**Рањивост**
Корпоративна мрежа	Вирус (антивирусни софтвер није инсталиран, база потписа за детекцију вируса није ажурирана).
	Напади социјалним инжењерингом (фишинг, лажна приступна тачка).
Логички контролни слој	Рањивости конфигурације (користи се подразумевана конфигурација система, критичне конфигурације се не чувају или немају резервне копије, безбедносне закрпе се не примењују редовно над ОС и апликацијама).
	Безбедносне слабости архитектуре (мрежна баријера, систем за детекцију упада није инсталиран)
	Рањивости софтвера (напади прекорачења бафера, DoS напади)
Физички контролни слој	Рањивости комуникације (коришћење несигурних ИКС протокола попут DNP3 или Modbus)
	Рањивости хардвера (несигуран даљински приступ компонентама ИКС, неадекватна физичка заштита критичних система и неовлашћено особље има физички приступ опреми)

TCP/IP рањивости могу бити искоришћене за пресретање контролних порука, захтевање основних, прислушкивање осетљивих информација о процесу, убацивање злонамерних команди за извршавање неодговарајућих акција или приказивање лажираних вредности. Противник такође може заобићи безбедносне механизме да уђе у систем и да изврши многе друге типове напада као што су читање/измена фајлова, праћење меморије и покретање сервиса користећи лажне команде. Протоколи за SCADA системе такође имају рањивости. На пример, комуникација Modbus/TCP се преноси у обичном тексту, омогућавајући великим деловима података (нпр. информације о постојећим инсталацијама и мрежним адресама) да буду манипулисани. Недостаје и механизам аутентификације јер Modbus сесије само проверавају валидност одређених делова поруке као што су адреса и функционални код. Протокол DNP3 такође има сигурносне недостатке иако укључује цикличну проверу грешака (енг. *cyclic redundancy check*, CRC), синхронизацију података и више формата података. SecureDNP3, варијанта DNP3, имплементира систем изазов-одговор аутентикације заједно са сесијским кључем за верификацију извора порука. ICCP такође има ограничења у вези са аутентификацијом и енкрипцијом.

Дијаграм модела претњи токова података референтног система је представљен на слици 10. За анализу рањивости коришћен је алат Microsoft Threat Modeling Tool [91]. Због поједностављења дијаграма, сервиси MDS, OMS, SMS су моделовани као Основни сервис, веб сервер, SMMS, INT као Јавни сервиси јер имају исте токове података па самим тим су на њих применљиве исте рањивости. Након цртања дијаграма, изгенерисан је извештај користећи алат да би се дошло до скупа рањивости система и његових компоненти. Ова анализа је кључна јер добијени извештај садржи генеричке рањивости од којих неке нису применљиве на ИКС. На основу искуства аутора, истраживања, прочитане литературе на тему претњи у ИКС, микросервисном архитектуром и системима у рачунарском облаку дефинисан је скуп рањивости, њихов утицај, вероватноћа па самим тим и ризик.



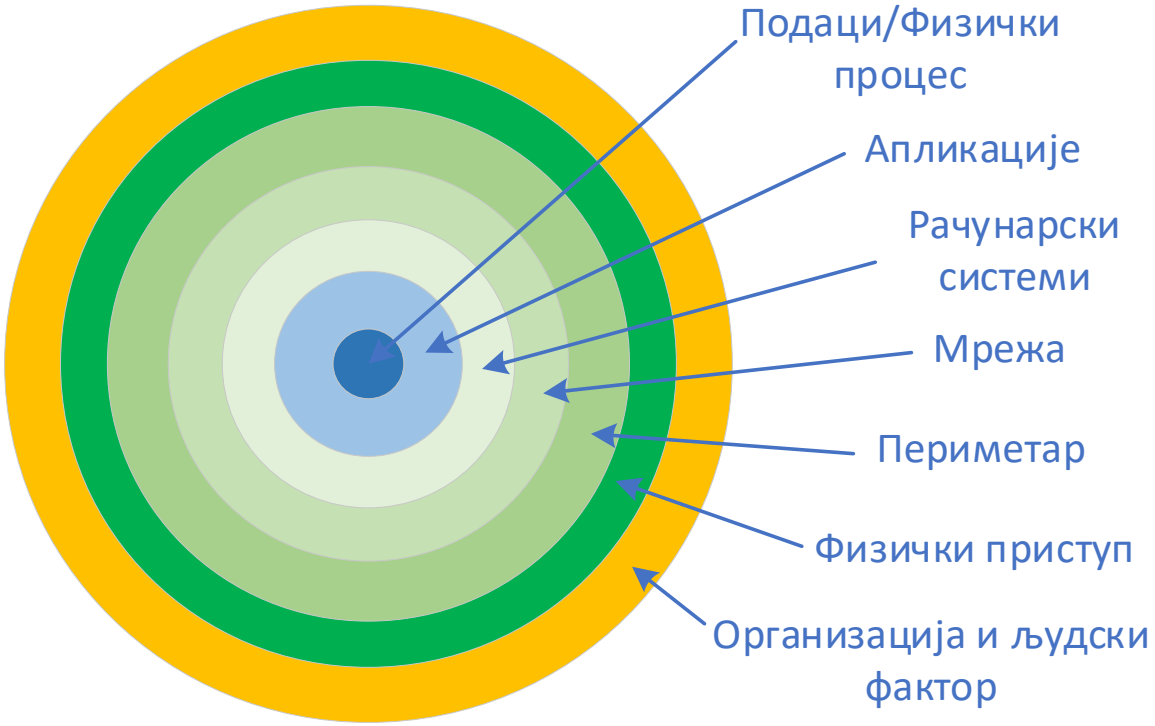
Слика 10 – Модел претњи референтне архитектуре

У наставку је презентован резултат спроведене анализе, односно списак рањивости:

Група	**Рањивост**
Лажирање	Лажиран клијент ако су коришћени слаби аутентификациони канали.
	Лажиран чвор коришћењем украденог сертификата.
Неовлашћено мењање	Неовлашћен приступ и измена порука и података чији интегритет није заштићен и који нису енкриптовани у преносу и у складишту.
	Искоришћење недостатка система за праћење и изазвати нежељени саобраћај ка бази података.
	Искључење система за надзор или извршавање манипулације над записима.
Одбацивање	Ускраћивање акције на бази података због недостатка надзора.
	Компровитовање безбедносних механизама базе података и спречавање извршења валидне акције.
Откривање информација	Приступ осетљивим подацима из базе података преко убацивања SQL команди.
	Приступ осетљивим информацијама као што су креденцијали, сертификати и кључеви који се чувају у меморији процеса или у кешу оперативног система.
	Прислушкивање комуникационих канала и крађа тајни које се преносе незаштићеним каналима.
Ускраћивање услуга	DDoS напад ако ограничавање брзине приступа (енг. *throttling*) није омогућено.
Елевација привилегија	Неовлашћен приступ операцијама и ресурсима микросервисног кластера добијањем већих привилегија.
	Неовлашћени приступ бази података због недостатка заштите мрежног приступа и слабих правила ауторизације.

4. ПРЕДЛОГ БЕЗБЕДНЕ АРХИТЕКТУРЕ СИСТЕМА

Главна стратегија која се користи за безбедност ИКС је одбрана у дубину (енг. *defense in depth*) [92]. Принцип одбране у дубину се ослања на примену више слојева заштите, са циљем да се повећа отпорност на нападе. Уместо ослањања на један слој заштите, овај приступ подразумева употребу различитих мера и механизама на свим нивоима система, од мреже и апликација до корисничког приступа. Сваки слој функционише као додатна баријера, тако да чак и ако један слој буде компромитован, остали слојеви настављају да пружају заштиту. Ово присиљава потенцијалног нападача да уложи више времена, ресурса и вештина како би пробио све нивое одбране, чиме се повећава вероватноћа за откривање и спречавање напада [93].



Слика 11 – Одбрана у дубину [89]

На слици 11 су приказани сви нивои одбране у дубину и у наставку су побројане методе које је потребно имплементирати на сваком нивоу [89]. ***Организација*** обухвата обуку, подизање свести и управљање ризицима. ***Физичка безбедност*** укључује физичку заштиту уређаја који се налазе на терену и у власништву компаније, док је физичка заштита ресурса у рачунарском облаку одговорност пружаоца услуга рачунарског облака.

Периметар подразумева мрежну баријеру и VPN тунел. ***Мрежа*** обухвата сегментацију мреже, IPsec и систем за откривање упада у мрежу. ***Рачунарски системи*** захтевају побољшање безбедности оперативног система, редовна ажурирања, аутентификацију и систем за откривање упада. ***Апликације*** укључују антивирус и конфигурацију, док ***подаци*** захтевају листу за контролу приступа и енкрипцију.

Имплементација принципа одбране у дубину је мало другачија за системе који се налазе у рачунарском облаку јер безбедност на неким нивоима постаје дељена одговорност. Модел дељене одговорности (енг. *Shared Responsibility Model*) се односи на поделу безбедносних, сигурносних и одговорности које су везане за приватност података између пружалаца услуга рачунарског облака и корисника услуга (организација које користе рачунарски облак). Овај модел је описан у смерницама NIST SP 800-144, NIST SP 800-145 и NIST SP 500-292 [75, 76, 74]. Одговорност је другачија у зависности од тога који модел рачунарског облака се користи. Модел од интереса у овој докторској дисертацији је PaaS:

- ***Корисник*** је одговоран за интегритет и безбедност података, то укључује контролу приступа подацима, енкриптовање података и управљање идентитетима који имају приступ подацима. Поред података, корисник је одговоран и за безбедност апликације. Предлог је да усвоји циклус развоја безбедног софтвера (енг. *Security Development Lifecycle*, SDL) како би осигурао да су све рањивости апликације идентификоване и решене.

- Одговорности **пружаоца услуга** укључују обезбеђивање физичке сигурности сервера, инфраструктуре мреже, хардвера и основне софтверске платформе. Води рачуна о безбедности мреже штитећи је од проблема као што су дистрибуирани напад ускраћивања услуге (енг. *Distributed Denial of Service,* DDoS), напади "човек у средини" (енг. *Man-in-the-Middle,* MitM), лажно представљање IP адреса, скенирање портова или прислушкивање пакета. Управљање идентитетима из угла приступа ресурсима у рачунарском облаку је такође задатак пружаоца услуга. Што се тиче безбедности сервера, пружалац услуга треба редовно да примењује безбедносне закрпе на своје ресурсе.

Још један принцип који је потребно имплементирати како би се спречили напади од инсајдера је принцип нултог поверења [29]. Детаљан опис овог принципа је дат у додатку Ц. Принцип нултог поверења налаже да ниједан корисник или сервис, било да је интерни или екстерни, не добија аутоматско поверење. Уместо тога, сваки приступ се третира као небезбедан и захтева верификацију идентитета, контролу приступа и праћење активности. Неколико кључних разлога зашто је добро имплементирати овај принцип нултог поверења у ИКС:

- Уводе се нови слојеви заштите који контролишу приступ.

- У ИКС постоји велики број уређаја и сервиса који међусобно комуницирају. Принцип нултог поверења осигурава аутентификацију и проверу сваке комуникације између ових сервиса пре него што се дозволи приступ.

- ИКС су често мета и инсајдерских и спољашњих напада. Принцип нултог поверења приморава све кориснике и сервисе да прођу кроз проверу идентитета, смањујући

шансе за злоупотребу приступа чак и од стране легитимних, али компромитованих корисника.

- Приступ је ограничен само на оно што је неопходно за одређени задатак или процес.

- Заштита од бочног кретања (енг. *lateral movement*). Уколико се један део система компромитује, принцип нултог поверења спречава нападаче да лако пређу на друге делове система, јер сваки појединачни елемент система захтева поновну верификацију иденититета.

У овом поглављу доказана је следећа хипотеза:

Принцип нултог поверења је применљив у индустријским контролним системима.

4.1 Нефункционални безбедносни захтеви за критичне инфраструктуре

Нефункционални безбедносни захтеви односе се на карактеристике система које обезбеђују његову заштиту и интегритет, али нису директно повезане са конкретним функцијама које систем извршава. Ови захтеви утичу на перформансе, поузданост и безбедност система.

Слика 12 – Нефункционални безбедносни захтеви

У случају критичне инфраструктуре то су следећи захтеви (слика 12):

- ***Редунданција***: Кључне компоненте као што су људство, контролни центри, рачунарска инфраструктура, сервери, радне станице, софтвер (процеси) и подаци морају бити дуплиране. Овим се осигурава да ће систем наставити да функционише чак и ако дође до квара или оштећења једне компоненте или комуникационог канала.

- ***Безбедни протоколи***: Потребно је користити протоколе који су прихваћени индустријским стандардом и који обезбеђују да је систем заштићен од неовлашћеног приступа и злоупотребе. Један пример таквог протокола за комуникацију је TLS (енг. *Transport Layer Security*).

- ***Контрола приступа***: Строга контрола приступа је неопходна за регулисање ко може приступити компонентама система и шта може да уради. Ово укључује аутентификацију, ауторизацију корисника и принцип нижих привилегија. Ограничава се приступ корисницима само на оно што им је неопходно за њихов рад. Овим се смањује ризик од злоупотребе и неовлашћеног приступа.

- ***Сегментација мреже***: Систем треба поделити на сегменте или зоне са различитим нивоима безбедности и поставити мере безбедности на границе зона. Овим се спречава ширење рањивости и грешака из једног дела система у други.

- ***Континуирано надгледање и анализа безбедности***: Потребан је централни систем за надгледање безбедности који прати понашање система у реалном времену и шаље обавештења о потенцијалним инцидентима или неправилностима.

- ***Заштита података и енкрипција***: Мора да се осигура да су сви подаци заштићени од неовлашћеног приступа, измене и брисања. Јака енкрипција је потребна за заштиту података у транзиту и током складишта. Због законских оквира, подаци не смеју да напусте регион у ком су настали.

- ***Опоравак од катастрофе***: Потребно је дефинисати компоненте, механизам за опоравак и очување система након озбиљних инцидената.

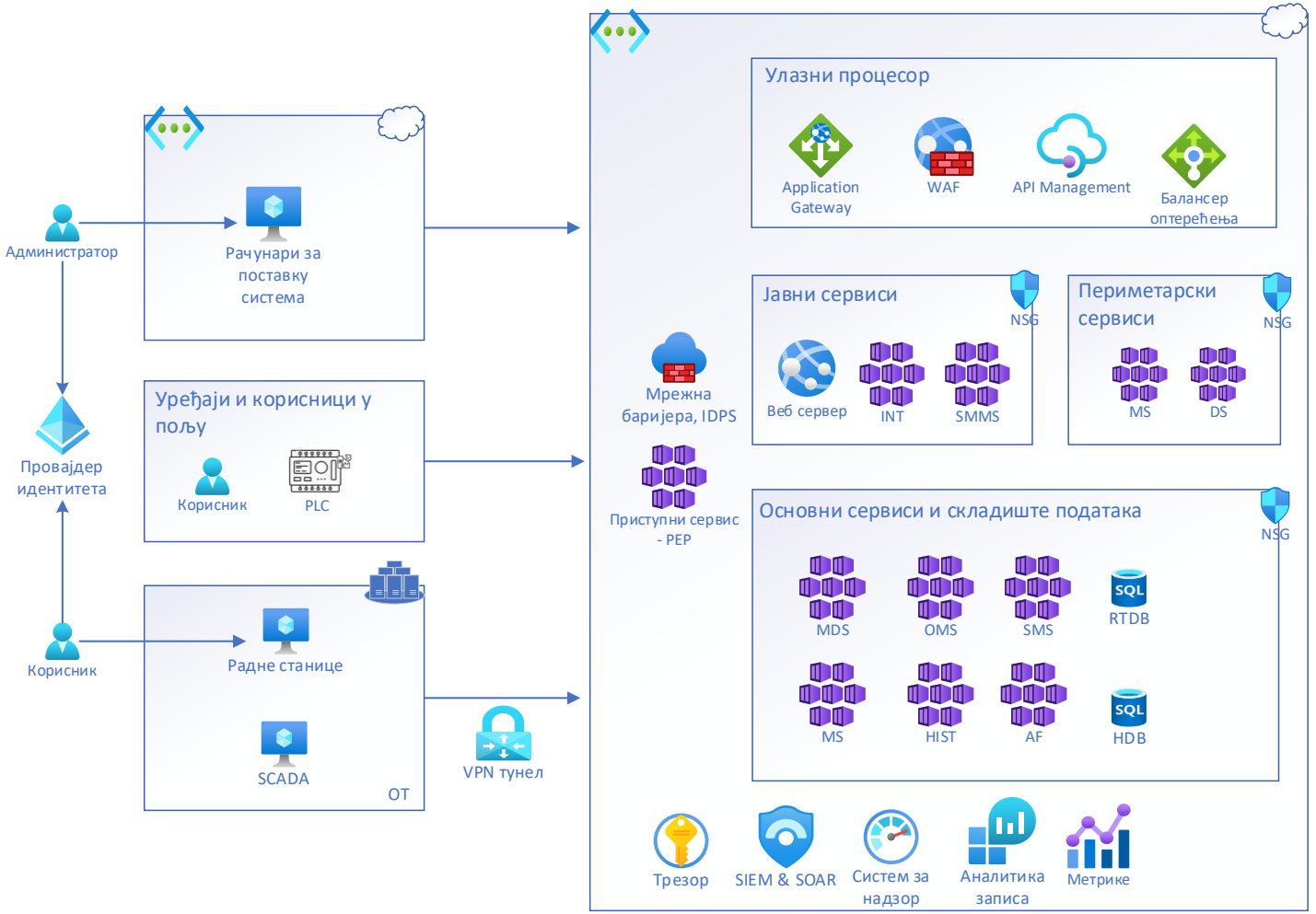
- ***Реакција на инциденте***: Организован процес одговора на безбедносне инциденте, као што су напади, грешке у систему или злонамерне активности. Циљ реакције на инциденте је његово ограничавање, уклањање и обнављање нормалног рада система, као и анализа узрока како би се спречило будуће понављање.

- ***Редовна анализа ризика***: Систематско процењивање ризика којима је организација изложена, на основу чега се идентификују потенцијалне рањивости система, као и могуће последице тих рањивости. Редовна анализа ризика омогућава организацији да одреди приоритет за имплементацију одређене мере заштите и да обезбеди управљање ризицима у складу са актуелним безбедносним претњама.

- ***Редовна пенетрациона тестирања***: Симулирани напади на систем, које спроводе безбедносни стручњаци како би открили рањивости у системима. Пенетрациона тестирања се користе за идентификовање и отклањање слабих тачака у систему пре него што их искористе стварни нападачи. Редовно спровођење оваквих тестирања помаже организацији да унапреди своју безбедност и осигура отпорност на нападе.

4.2 Примењене безбедносне мере у архитектури

Истраживањем литературе, безбедносних стандарда и смерница описаних у поглављу 2.3, описана референтна архитектура ОТ подсистема је проширена одговарајућим мерама безбедности и приказана на слици 13.



Слика 13 – Предложена безбедна архитектура система

У наставку су наведене сумиране главне измене архитектуре са слике 13 које ће бити објашњене у наредним поглављима:

- ***Мрежна сегментација*** – јавни, периметарски и основни сервиси су постављени у засебне подмреже између којих је имплементирана мрежна баријера. Оваква конфигурација мреже омогућава контролисану комуникацију између различитих делова система, да сваки пренос података може да се забележи у систему за надзор и изолацију појединих делова мреже у случају инцидента. Мрежна баријера је компонента која обезбеђује контролу и надзор саобраћаја унутар мреже. У случају архитектуре нултог поверења сва међусервисна комуникација пролази кроз мрежну баријеру. Додатак у односу на традиционалну мрежну баријеру је њена интеграција са системом за откривање и превенцију упада (енг. *Intrusion Detection and Prevention System*, IDPS). Ова интеграција повећава ефикасност заштите, јер омогућава рано откривање и брзу реакцију на потенцијалне сајбер претње.

- ***Улазни предпроцесор*** – састоји се од четири алата које пружа платформа рачунарског облака као SaaS решења. Њихов опис налази се у поглављу 4.1.7. Главна улога улазног предпроцесора је да обави иницијалну анализу и валидацију захтева пре него што се он проследи одговарајућим сервисима. Валидација подразумева проверу важећих сертификата како би се обезбедило да захтеви долазе од легитимних извора и инспекцију мрежних пакета у потрази за познатим нападима (укључујући покушаје инјекције злонамерног кода или других облика сајбер напада). У случају захтева који долазе од уређаја проверава се и да ли је уређај регистрован у систему.

- ***Сервис за контролу приступа*** – управља процесом аутентификације и ауторизације корисника и сервиса. Његова главна улога је да обезбеди да само овлашћени корисници или сервиси могу приступити ресурсима или сервисима унутар система. Коришћени протоколи за аутентификацију и ауторизацију OAuth2.0 и OpenID Connect (OIDC) описани су детаљно у додатку Е. Како је архитектура нултог поверења имплементирана, сервис за контролу приступа се позива и приликом међусервисне комуникације како би се утврдило да ли сервис има довољна права за извршавање функције другог сервиса. Сервис за контролу приступа прво проверава валидност токена који садржи информације о идентитету и правима приступа корисника или сервиса и представља доказ успешне аутентификације. Након валидације токена следи ауторизација где сервис за контролу приступа на основу дефинисаних полиса одлучује да ли корисник или сервис има одговарајућу привилегију за приступ траженим ресурсима или за извршавање одређених операција.

- ***Трезор*** – служи за безбедно чување осетљивих података као што су тајне, сертификати и кључеви за енкрипцију. Овај сервис омогућава приступ осетљивим подацима на контролисан и сигуран начин, уз јаку аутентификацију и енкрипцију. Кроз механизме ротације кључева и лозинки, трезор осигурава да се тајне ажурирају аутоматским, без људске интервенције, чиме се смањује ризик од компромитовања.

- ***Алати за надзор система*** – користе се напредни алати које нуди платформа рачунарског облака. Ови алати омогућују праћење рада и перформанси система у реалном времену. Неке од метрика које прикупљају и анализирају су коришћење ресурса (процесор, меморија, диск), мрежни саобраћај, стање сервиса, као и грешке и инциденти који се јављају током рада система. Њихова главна улога је да омогуће рано откривање проблема, као што су успорени процеси, грешке у сервисима или безбедносни инциденти. Поред тога, неки алати укључују механизме за аутоматско реаговање на одређене догађаје, као што су скалирање ресурса или обавештавање администратора о критичним инцидентима. Ови алати доприносе високој доступности, стабилности и сигурности система кроз континуирано праћење и превентивне мере.

- ***Аутоматско скалирање ресурса*** – системи са микросервисном архитектуром у рачунарском облаку могу аутоматски повећавати или смањивати ресурсе (нпр. број инстанци) у зависности од оптерећења. Ова функционалност омогућава систему да обрађује веће количине захтева током већих оптерећења, док се у време мање потражње ресурси оптимизују како би се смањили трошкови и сачувала ефикасност. Додатно, коришћењем компоненте за расподелу оптерећења, саобраћај се равномерно дистрибуира између различитих инстанци микросервиса, чиме се смањује ризик од преоптерећења било које појединачне инстанце.

На слици 13 је приказано све претходно наведено. Тиме је доказана следећа хипотеза:

Могућ је развој безбедне архитектуре индустријског контролног система базираног на микросервисима у рачунарском облаку.

4.2.1 Успостављање строгих правила администрације

Иако већ постоје, правила за коришћење система морају бити ревидирана и по потреби допуњена [94]. Морају бити имплементиране одговарајуће контроле запослених који имају приступ ресурсима система, његовој архитектури, изворном коду и подацима. На пример, запослени морају бити обучени из угла безбедности и поседовати одговарајуће сертификате. Радње као што су инсталација система, креирање ресурса, извршавање ажурирања морају бити потпуно аутоматизоване и спроведене из безбедног окружења. Ручне измене над конфигурацијом система треба да буду сведене на минимум и да се спроводе само у екстремним ситуацијама, као што је спречавање неког напада. Сваки приступ ресурсима у администраторске сврхе или извршавање ручне измене мора бити извршен са администраторског налога који је додатно заштићен и праћен. Ниједан кориснички налог, па ни администраторски, не сме да има највише привилегије подешене као подразумеване. Потребно је користити алат који омогућава елевирање привилегија на одређени временски период у току ког се обављају радње које захтевају више привилегије. Приликом подношења захтева за елевацију привилегија, мора бити објашњен разлог тражења приступа након чега глобални тим одобрава или одбија захтев.

Приступ ресурсима у рачунарском облаку је потребно имплементирати коришћењем сигурних канала и сервиса. *Just-In-Time* (JIT) представља безбедносну праксу која корисницима омогућава приступ ресурсима само када је то заиста потребно, за време које је потребно да се задатак изврши и само са одређених адреса. Провајдери услуга у рачунарском облаку омогућавају да се подесе полисе које ће да захтевају да су радне станице које се користе за приступ ресурсима управљане од стране компаније као и да се ресурсима може приступити само са одређене локације или региона. Ово је важно због захтева да подаци не смеју да напусте регион (GDPR, ISO/IEC 27018) и да се систему може приступити само из региона у ком су инсталирани.

4.2.2 Аутентификација и ауторизација

Било каква врста анонимног приступа, у административне или корисничке сврхе мора бити онемогућена. Препорука је да се користе протоколи OIDC и OAuth2.0 за аутентификацију и ауторизацију што и јесте стандард за микросервисне архитектуре. Провајдер идентитета (енг. *Identity Provider*, IdP) потврђује идентитет корисника и управља њиме. Корисници морају да се аутентификују пре него што добију дозволу приступа систему, односно приступни токен (енг. *JSON Web Token*, JWT). Кроз полисе на провајдеру идентитета се дефинишу правила као што су обавезно коришћење јаких лозинки, обавезна вишефакторска аутентификација (енг. *Multi-factor Authentication*, MFA), дозвољена приступна локација и захтеви који се примењују на радну станицу са које се приступа. Оваквом имплементацијом, нападач не може да добије токен чак и ако украде корисничку лозинку. У провајдеру идентитета могу да се дефинишу и права приступа систему. Користећи ток ауторизационог кода (енг. *Authorization Code Flow*), клијентска апликација преусмерава корисника на страницу за пријављивање провајдера идентитета, а затим се након успешне аутентификације добија ауторизациони код. Клијентска апликација затим користи тај код за добијање приступног и токена за освежавање (детаљнији опис у додатку Е). Приступни токен се користи за ауторизацију јер се у њему налазе сва права приступа корисника. Токен за освежавање је пожељно користити како би се приступни токен могао обновити када истекне без потребе да клијент поново уноси своје креденцијале.

Да би се систем заштитио од инсајдерских претњи, потребна је имплементација принципа нултог поверења, односно аутентификација свих компоненти система. За комуникацију између микросервиса, препорука је да се користи ток клијентских креденцијала (енг. *Client Credentials Flow*). За имплементацију овог тока, потребно је регистровати микросервис у провајдеру идентитета. Микросервиси се аутентификују провајдеру идентитета користећи јединствени идентификатор и тајну која одговара регистрованој апликацији (детаљнији опис у додатку Е). Након аутентификације добија се приступни токен који се користи за ауторизацију. На исти начин је имплементирана и аутентификација SCADA система који се налази у контролном центру (тј. није у рачунарском облаку).

Коришћење различитих администраторских алата који комуницирају са системом је такође заштићено тако што је обавезна аутентификација администратора приликом покретања алата. Користи се исти принцип као код аутентификације крајњих корисника. Корисник након успешне аутентификације добија приступни токен који се даље користи за ауторизацију.

Из претходно наведеног, може се закључити да постоје различити сценарији коришћења система:

- приступ корисника систему,
- приступ систему у сврху инсталације и конфигурације,
- администраторски приступ и
- међусервисни приступ.

За имплементацију принципа нултог поверења сваки микросервис мора да проверава права приступа позиваоца његових услуга. Контрола приступа заснована на улогама (енг. *Role-based Access Control*, RBAC) мора бити имплементирана пратећи принцип нижих привилегија. За сваки сервис је потребно дефинисати које пермисије су потребне да би се извршила одређена операција. По архитектури нултог поверења, ова конфигурација се дефинише полисама где једна полиса одговара једној сервисној операцији. Приликом позива сервисне операције, као део заглавља шаље се одговарајући токен. Микросервиси су одговорни за проверу валидности токена. Након што је утврђено да је токен валидан, позива се приступни сервис (енг. *access service*) како би се утврдило да ли корисник има права да изврши затражену операцију (детаљнији опис у додатку Ц). Поред провере валидности токена и асоцираних пермисија, коришћењем интеграције са алатима као што су алат за управљање безбедносним информацијама и догађајима (енг. *Security Information and Event Management*, SIEM) и алат за управљање привилегованим приступом (енг. *Privileged Access Management*, PAM), приступни сервис проверава да ли је за корисника везан неки инцидент, да ли му је приступ повучен или је означен као ризичан. У случају да је било шта од претходно наведеног испуњено, кориснику ће бити одбијен приступ. Још један принцип који је пожељно импелементирати код система микросервисне архитектуре је принцип поделе одговорности. Овим се осигурава да корисници и развојни тимови имају различите улоге и одговорности које се не преплићу што спречава злоупотребу у развоју и одржавању система.

4.2.3 Заштита тајни и података

Истраживања су показала да недостаје криптографија у ИКС кад су у питању подаци, аутентичност ентитета и поверљивост података [95]. Такав јаз омогућава једноставне нападе попут имитације уређаја и прислушкивања комуникационих канала. Стога је потребно укључити ефикасне криптографске механизме, проверу интегритета и аутентичности података у реалном времену.

Нису сви подаци у систему исте важности, и због тога је потребно разликовати нивое осетљивости података како би се применио одговарајући ниво заштите. Осетљиви подаци или тајне које чувају сервиси морају бити енкриптовани и енкрипција на нивоу диска мора бити коришћена. За складиштење тајни, сертификата и кључева треба користити трезор, као решење које има сопствену аутентификацију и ауторизацију. Време током ког се осетљиви подаци чувају у систему је потребно ограничити. Подаци који више нису потребни треба да буду безбедно обрисани како би се смањио ризик од њиховог откривања у случају компромитовања система.

Податке не сме да види и да им приступи нико без права и све тајне морају да се чувају коришћењем индустријских алгоритама и одговарајућих дужина кључева. Рачунарски облак коришћењем виртуализације уводи нову рањивост јер сада више виртуелних ресурса користе један физички. Ово оставља могућност за извођење софистицираног напада где један процес може да сруши баријеру и приступи меморији другог процеса. Поред енкриптовања осетљивих података у меморији, препорука је користити и хардверску заштиту, односно поверљиво рачунарство (енг. *Confidential Computing*), како би се спречило цурење (екфилтрација) осетљивих података док су у употреби.

Листе контроле приступа (енг. *Access Control Lists*, ACL) морају бити имплементиране над фолдерима и датотекама (нпр. XML датотеке) како би се спречила њихова неовлашћена манипулација. Поред тога, битна је и провера интегритета фајлова која се постиже потписивањем датотека са кључем чији јавни део имају и сервиси који могу да провере да ли је датотека потписана валидним сертификатом. Ручна измена мењање осетљиве конфигурације мора да буде забрањена. Када је у питању конфигурација која није осетљива, да би извршио ручно ажурирање, администратор мора да тражи додатна права коришћења од сервиса за управљање приступом и да приликом приступа ресурсу понови вишефакторску аутентификацију.

Обавезан је бекап свих података како би се осигурала њихова заштита и доступност у случају губитка, оштећења или компромитације оригиналних података. Ове копије се морају чувати на безбедној локацији, физичкој или у облаку, и могу се користити за враћање података у првобитно стање у случају инцидента.

4.2.4 Безбедност мреже

Анализом шаблона мрежног саобраћаја и понашања система, машинско учење доприноси откривању рањивости у реалном времену [95]. Потребно је користити систем за откривање упада који ради по принципу нултог поверења. Овим се примењује свеобухватан приступ за континуирану валидацију и праћење мрежних активности, обезбеђујући идентификацију и ублажавање потенцијалних безбедносних пропуста како из унутрашњих, тако и из спољашњих извора.

Што се тиче комуникације између сервиса, ограничавање брзине приступа (енг. *throttling*) треба да буде подешено. По принципу нултог поверења, потребно је користити мрежну баријеру како на самом улазу у систем тако и између његових компоненти. Он служи као прва линија одбране и блокира неовлашћен саобраћај на основу утврђених правила. Мрежни саобраћај треба да буде дозвољен само са одређених адреса и портова. У рачунарском облаку препорука је да се користи мрежна баријера која поред своје основне функције има и интегрисан IDPS. Захваљујући дубинској инспекцији пакета (енг. *Deep Packet Inspection*, DPI), анализира сваки пакет, како на нивоу заглавља тако и на нивоу садржаја, што омогућава препознавање сложених или скривених напада.

Мрежна сегрегација је важна за одвајање сервиса који имају комуникацију са екстерним системима од остатка система. Свака мрежна група има дефинисана улазна и излазна мрежна правила, што је још један слој ограничења комуникације између сервиса. Спречавање прекомерне потрошње (енг. *over-consumption*) ресурса ограничавањем истовремених позива, инстанци или сесија је такође добра пракса.

Сервиси не смеју да буду јавно изложени нити да имају јавне крајње тачке (енг. *endpoints*). У случају потребе приступа са јавног интернета неком сервису, обавезно је коришћење HTTPS и захтев мора да прође обраду кроз улазни процесор (слика 13).

4.2.5 Безбедност базе података

Приступ бази података треба да буде конфигурисан помоћу корисничких група (енг. *roles*) и налози са најмањим привилегијама (енг. *least-privileged accounts*) да се користе за повезивање са базом података. Директни приступ табелама у бази података треба да буде онемогућен и да постоји листа изабраних ускладиштених процедура које сервиси могу да исвршавају. Контрола пријављивања треба да буде омогућена на серверу базе података за ограничену групу администратора. За енкрипцију података у бази података морају се користити јаки алгоритми за енкриптовање. У микросервисној архитектури, добра пракса је да сваки сервис има сопствену базу података тако да ризик од ометања података других није могућ. Ако то није могуће, мора се применити заштита на нивоу реда (енг. *Row Level Security*, RLS). Заштита на нивоу реда омогућава имплементацију ограничења приступа редовима у бази података где сервиси могу да приступе само оним редовима података који су релевантни за њихов опсег.

4.2.6 Вођење записа и надзор

Анализа корелације записа (енг. *log files*) различитих сервиса треба да се користи у ИКС мрежи како би се побољшало управљање инцидентима у међусобно повезаним сервисима. Одговарајуће евидентирање, уз обавезно укључивање временске ознаке (енг. *timestamp*), свих безбедносних догађаја и корисничких активности даје могућност праћења акција у систему. Сваки успешан и неуспешан покушај аутентификације и ауторизације мора бити забележен. Систем треба да евидентира сваки захтев кроз записе које се чувају у датотекама. Ове датотеке записа се сматрају осетљивим информацијама и треба да буду заштићене од неовлашћеног приступа ограничавањем привилегија писања на сервисе и прегледа на администраторе у сврху инспекције уколико дође до проблема. Још једна добра пракса је онемогућавање брисања ових датотека, као и њихово архивирање. Коришћење напредних алата на серверима је потребно како би се дефинисале беле листе апликација које су дозвољене за покретање. Ови алати уче понашање система и детектују било које одступање, на пример ако је нека нова апликација покренута која није на белој листи, она се третира као малициозна и одмах се шаље одговарајуће обавештење.

Како би се утврдило шта је неуобичајено понашање система, потребно је најпре дефинисати параметре који се очекују у нормалном раду, укључујући перформансе, мрежни саобраћај, време потребно за одговор на захтев и друге релевантне индикаторе. Овим процесом се успостављају основни параметри за сваки аспект система, што омогућава да се одступање од тих вредности идентификује. За ефикасно праћење перформанси ИКС и одржавање робусних мера безбедности потребно је имплементирати праћење следећих параметара [95]:

- Записи догађаја морају се пратити и анализирати ради откривања неуобичајеног понашања система.

- Прикупљање мрежних података може се користити за истраживање понашања мреже. Пасивно прикупљање не утиче на критичне системе и не изазива кашњење у услугама.

- Подаци генерисани са уређаја у ОТ мрежи треба да буду видљиви аналитичарима безбедности.

Праћење системских метрика такође може бити корисно у откривању неуобичајеног понашања система. На пример, нагло повећање броја инстанци сервиса би могао бити индикатор да је напад у току. Поред броја захтева и броја инстанци сервиса, следеће метрике могу такође бити корисне: успешне/неуспешне пријаве на систем, приступ трезору, трајање извршавања захтева, коришћење CPU/меморије за сваки сервис, саобраћај између компоненти система, приступи бази података.

SIEM је препоручен алат који поред праћења записа доноси и детекцију претњи анализом прикупљених безбедносних догађаја. Уз њега иде и алат за безбедносну оркестрацију, аутоматизацију и одговор (енг. *Security orchestration, automation and response,* SOAR). Заједно ова два алата представљају јединствено решење за откривање напада, видљивост претњи, проактивну детекцију напада и одговор на претње. Препорука је да се сви безбедносни записи преносе у рачунарски облак где се могу користити већ постојећи SaaS алати. Ови алати могу да се подесе тако што ће да реагују на свако одступање од нормалног понашања система тако што креирају инцидент одређеног типа. Тим за безбедносне операције (енг. *Security Operations Center,* SOC) треба да прати активности на систему 24/7.

4.2.7 Заштита од екстерног периметра

Посебна пажња је потребна за уређаје у пољу који комуницирају директно са системом преко веб сервиса. Сваки уређај мора да поседује сертификат због идентификације. Сертификати морају бити потписани од стране одобреног ауторитета за издавање сертификата (енг. *Certificate Authority,* CA), а самопотписани или тестни сертификати нису дозвољени у продукционим окружењима. Поред сертификата, потребно је имплементирати посебну процедуру регистрације уређаја приликом које се јединствени идентификатор уређаја уноси у модел. Веб-базирани сервиси нису директно изложени јавном интернету већ постоје компоненте које обрађују захтев пре него што се он пропусти до њих:

- ***Application Gateway*** је врста мрежног уређаја који обезбеђује управљање саобраћајем на нивоу апликација (OSI слој 7). Проверава валидност сертификата и одбија захтеве који имају невалидан сертификат. Омогућава усмеравање саобраћаја у зависности од заглавља HTTP захтевима, као што су URI путање. Треба да буде подешен тако да захтева HTTPS, врши функције као што су SSL терминирање и има уграђену заштиту од DDoS напада.

- ***Web Application Firewall (WAF)*** је специјализовани облик мрежне баријере који филтрира, прати и блокира HTTP саобраћај према и од веб сервиса. WAF штити веб апликације од напада који искоришћавају познате рањивости као што су SQL инјекција, cross-site scripting (XSS), укључивање датотека (енг. *file inclusion*) и неправилну конфигурацију система. WAF примењује ограничења на број захтева од одређене IP адресе или географске локације, што помаже у идентификацији и блокирању злонамерних напада.

- ***API Management*** је компонента која омогућава креирање, објављивање и управљање интерфејсима, контролу приступа, праћење њихове употребе и

спровођење безбедносних полиса. Његовим коришћењем, позиви ка невалидним интерфејсима су одбијени пре него што дођу до сервера. Приликом обраде захтева, API Management провери да ли уређај постоји у моделу и да ли је његов сертификат исправан.

- ***Балансер оптерећења (енг. Load Balancer)*** је компонента која распоређује саобраћај преко више инстанци микросервиса, чиме се обезбеђује да је оптерећење изједначено и да у случају пада једне инстанце друге преузму оптерећење. Иако платформа за оркестрацију обавља расподелу саобраћаја унутар микросервисног кластера, екстерни саобраћај који долази изван кластера (нпр. од корисника) захтева постављање екстерног балансера оптерећења.

Сигуран канал (енг. *site-to-site* VPN) који је енкриптован мора бити отворен између контролног центра и рачунарског облака. За отварање овог канала користе се посебне компоненте које се зову *VPN Gateway* (слика 13). Сервиси треба да прате учесталост промена вредности и ако неки теренски уређај шаље више промена него обично, инцидент треба да се пријави са високим приоритетом. SIEM се може користити као алат за детекцију у овом сценарију.

4.2.8 Сигурна поставка система

За поставку система потребно је подићи посебну, управљачку зону у рачунарском облаку. У овој зони треба да буду рачунари на којима су инсталирани алати који служе за постављање система као и сигурне базе података које се користе за пренос инсталација, сертификата и конфигурације. Сама поставка система и креирање ресурса мора бити аутоматизована у што већој мери. Приступ рачунарима је ограничен само за администраторе.

Потребно је користити систем који ће да омогући аутоматизован процес креирања, издавања, дистрибуције, складиштења, обнављања и опозива сертификата. Систем треба да има евиденцију свих сертификата како би могао да прати њихов статус и рок важења и благовремено изврши њихову обнову. Што се тиче складиштења, сертификати треба да буду сачувани искључиво у трезору где ће приступ бити омогућен само сервисима који их користе. Још једна битна функционалност је опозив сертификата који је компромитован или више није безбедан како би се спречила његова злоупотреба.

4.2.9 Одговор на инциденте

Израда плана за одговор на инциденте почиње планирањем и припремом, укључујући формирање тима за одговор на инциденте, дефинисање полиса, постављање комуникационих протокола и обезбеђивање функционалности. Алат SOAR може значајно да побољша ефикасност и брзину одговора на сајбер инциденте јер може да координише различитим безбедносним алатима, као што су SIEM, IDS/IPS, антивирусним програмима и слично. Битна ставка је могућност аутоматизације рутинских задатака, као што су блокирање IP адресе или изолација компромитованог уређаја. Ово омогућава брзо реаговање на инциденте кроз дефинисање и извршавање унапред припремљених скрипти (енг. *playbook*) које садрже кораке које треба предузети да би се инцидент решио на најефикаснији начин. Како се напади стално развијају и постају све софистицираниј тако треба увести и континуирано побољшавање процедура и одговора на инциденте у складу са анализом претходних инцидената. Зато је битно прикупљати податке током инцидената

и генерисати детаљне извештаје. Ови извештаји такође могу послужити као основа за праћење усклађености са регулативама и стандардима безбедности.

Један пример плана за одговор на инцидент употребом алата:

1. Детекција инцидента: SIEM систем детектује необичну активност на мрежи.
2. Аутоматизована реакција: SOAR аутоматски покреће скрипту која укључује скенирање компромитованих система, блокирање IP адресе и обавештавање безбедносног тима.
3. Оркестрација ресурса: SOAR координира активности између различитих безбедносних алата, као што су антивирусни програми и IDS/IPS системи.
4. Извештавање: Након завршетка инцидента, SOAR генерише детаљан извештај који садржи све кораке који су предузети, анализу узрока инцидента и препоруке за будуће мере предострожности.

5. ВЕРИФИКАЦИЈА БЕЗБЕДНОСТИ ПРЕДЛОЖЕНЕ АРХИТЕКТУРЕ

Извршена је анализа сваке компоненте система из угла безбедности како би се одредио ниво безбедности предложене архитектуре. Систематски преглед литературе идентификује да је STRIDE [96] методологија најчешће коришћена техника за анализу рањивости у ИКС [97]. STRIDE, што је скраћеница за лажирање (енг. *Spoofing*), неовлашћене измене (енг. *Tampering*), одбацивање одговорности (енг. *Repudiation*), откривање информација (енг. Information *Disclosure*), ускраћивање услуге (енг. *Denial of Service*), и елевација привилегија (енг. *Elevation of Privilege*), широко је прихваћена због свог свеобухватног приступа анализи безбедносних својстава различитих компоненти система. Ова методологија оцењује безбедност архитектуре система користећи дијаграме тока података и идентификује могуће сајбер претње.

Рачунање ризика је засновано на два кључна фактора: утицају (табела 5), који се односи на могућу штету или последице по систем или организацију, и вероватноћу (табела 6), коришћења рањивости за извршавање успешних напада. Комбинацијом ових фактора добија се процена ризика (табела 7) која је јако важна за одређивање којим приоритетом ће се приступити решавању идентификованих рањивости.

Табела 5 – Утицај [29]

Утицај	**Опис**
Веома висок	Очекивани озбиљни или катастрофални негативни ефекти на рад, имовину, појединце: • Озбиљне повреде особља или губитак живота. • Дуготрајна недоступност и неупотребљивост система. • Уништење вредне имовине.
Висок	Свака радња која може довести до губитка клијената због непоузданости система и великог финансијског губитка: • Систем губи способност да изврши једну или више својих примарних функција и даје погрешне прорачуне. • Цурење тајних информација о клијентима. • Скупо оштећење опреме.
Средњи	Очекује се озбиљан нежељени ефекат: • Изазива значајну деградацију ефикасности функција система. • Губитак поверења клијената. • Откривање информација о систему које конкуренција (или нападач) може користити да би стекла предност. • Недоступност некритичних компоненти система.
Низак	Очекује се ограничени нежељени ефекат: • Мања штета на имовини. • Финансијски губитак.
Веома низак	Очекују се занемарљиви нежељени ефекти који не утичу на рад система.

Табела 6 – Вероватноћа [29]

Вероватноћа	**Опис**
Веома висока	Готово је сигурно да ће нападач искористити рањивост. То значи да систем има озбиљне безбедносне пропусте који се могу искористити, на пример, ако је систем јавно доступан и свако може да користи његове функције или мења податке.
Висока	Велика је вероватноћа да ће нападач искористити рањивост. Архитектура система има слабе тачке које искусни нападач може да искористи. Запослени са већим привилегијама него што је потребно може бити слаба тачка, било злонамерни (инсајдерска претња) или необразован и преварен од стране нападача.
Средња	Вероватно је да ће нападач искористити рањивост. Уз велики напор нападач може добити ограничен приступ систему, али и даље не може угрозити систем, па је његова мотивација ниска.
Ниска	Мало је вероватно да ће нападач искористити рањивост. Запослени су лојални и добро информисани о најновијим претњама, тако да се инсајдерске претње вероватно неће десити. Систем је заштићен на свом периметру, тако да ако дође до напада, нападач не може доћи до осетљивих информација.
Веома ниска	Мало је вероватно да ће нападач искористити рањивост. Систем је адекватно заштићен.

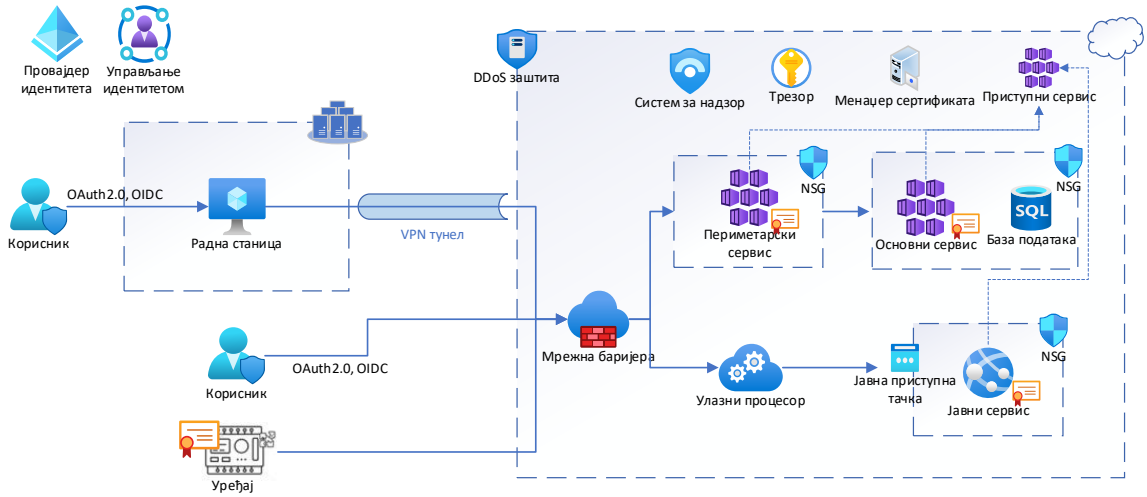
Табела 7 – Ризик [29]

	Утицај					
Вероватноћа		**Веома висок**	**Висок**	**Средњи**	**Низак**	**Веома низак**
	Веома висока	Веома Висок	Висок	Средњи	Низак	Веома низак
	Висока	Веома Висок	Висок	Средњи	Низак	Веома низак
	Средња	Висок	Средњи	Средњи	Низак	Веома низак
	Ниска	Средњи	Низак	Низак	Низак	Веома низак
	Веома ниска	Низак	Низак	Веома низак	Веома Низак	Веома низак

Ако је нека рањивост означена као висок ризик, систем може наставити са радом али одговарајуће мере морају бити имплементиране што пре. Према NIST и MITRE, ове рањивости треба да буду решене у року од пар сати до пар дана [98]. За рањивости средњег ризика, од пар дана до пар недеља и ниског нивоа до пар месеци где се решење обично испоручује кроз регуларан процес одржавања система.

5.1 STRIDE анализа компоненти система

У овом поглављу, свака компонента система са слике 13 се анализира појединачно коришћењем STRIDE методологије. Немају сви сервиси исти ниво критичности па самим тим ни рањивости над њима исти утицај тако да је анализа извршена за три категорије – јавни, периметарски и основни сервиси. На слици 14 су представљени детаљније токови података са препорученим мерама безбедности.



Слика 14 – Токови података безбедне архитектуре

5.1.1 Лажирање

У лажирању, комуникација која долази од непознатог извора је маскирана тако да изгледа као да је извор познат. Најслабија карика су запослени које нападач потенцијално може искористити коришћењем фишинга (енг. *phishing*), наводећи их да инсталирају злонамерни софтвер или открију поверљиве информације (нпр. њихову лозинку). Још један потенцијалан напад је лажирање сервиса у микросервисном кластеру. Нападач би могао компромитовати интегритет система убацивањем злонамерног сервиса који имитира легитимни, омогућавајући му да измени или манипулише подацима, прати рад система или онемогући извршавање критичних операција.

На слици 14 су приказане мере које су заједничке за све сервисе:

- Сервис спроводи аутентификацију и ауторизацију (OAuth2.0, OIDC) сваког захтева, било да долази од корисника или другог сервиса. Примењен је принцип нултог поверења.
- Нови сервис се у систем може додати само приликом најављене и планиране процедуре поставке система за коју је потребно одговарајуће одобрење.
- Саобраћај је енкриптован коришћењем TLS/SSL тако да подаци не могу бити промењени током преноса.
- Интегритет докумената и порука се гарантује потписивањем сертификатима.

- Тајне су сакривене у трезору који је заштићен посебним системом провере идентитета и права приступа.

- Све активности над системом, захтеви и одговори система се прате и снимају у централно место за надзор.

- Користи се аутоматски систем за управљање сертификатима чиме се обезбеђује да сви микросервиси користе актуелне и важеће сертификате. Украдени сертификат се поништава.

- Мрежа је сегментирана тако да се јавни, периметарски и основни сервиси налазе у посебним опсезима на чијим улазима се налази мрежна баријера са интегрисаним IDPS системом.

Ако нападач лажирањем добије приступ основном сервису он може да шаље команде на терен, креира инциденте, поништава аларме, мења историју и слично што по табели 5 спада у категорију веома високог утицаја. Додатна мера за ове сервисе је то да они немају јавну тачку приступа, приступ је могућ једино користећи клијентску апликацију преко сервиса који се налазе на периметру система где сав саобраћај пролази кроз више нивоа инспекције. Уведено је правило на мрежној баријери да сервису може да се приступи само са једне адресе, уз одговарајући сертификат и приступни токен. Периметарски сервиси врше додатну анализу захтева како би утврдили његову валидност.

Сервиси који су означени као периметарски имају посебну улогу у систему и они такође немају јавну тачку приступа али комуницирају директно са клијентском апликацијом и SCADA системом. Исто као и за основне сервисе, утицај је веома висок уколико се рањивост лажирања експлоатише. Предузета безбедносна мера је коришћење радних станица са којих корисници приступају систему које су физички изоловане, заштићене и у мрежи која је спојена са системом преко VPN канала. Приступне тачке су видљиве само машинама у клијентској мрежи. Због примене приступних полиса, платформа рачунарског облака ће да одбије захтеве са свих радних станица које нису у дефинисаном региону и које нису инсталиране од стране клијента. Такође, због употребе вишефакторске аутентификације, сама лозинка није довољна да се нападач улогује на систем чиме се штити клијентска апликација.

На крају остају јавни сервиси који имају јавну тачку приступа и служе за комуникацију са уређајима у пољу или корисницима који приступају са удаљених локација. Скуп операција које ови сервиси могу да изврше је мањи и не садржи критичне операције па је самим тим утицај њихових рањивости висок уместо веома висок као код претходних сервиса. Због обезбеђивања ове групе сервиса убачена је још једна компонента у архитектуру система која се зове улазни процесор и садржи четири алата које нуди рачунарски облак. Улога улазног процесора из контекста лажирања је да утврди валидност извора провером сертификата, адресе, инспекцијом садржаја и заглавља поруке. Поред тога ради и проверу да ли уређај који шаље захтев заиста постоји у систему.

Анализирајући спроведене мере, долазимо до закључка да је вероватноћа за лажирање веома ниска тако да је према матрици ризика представљеној у табели 7, ризик за ову рањивост **низак**.

5.1.2 Неовлашћене измене

Неовлашћена промена података који се налазе у бази података која припада мрежном сегменту основних сервиса, било да се ради о њиховом уништавању, манипулацији или изменама преко неовлашћених канала. Утицај ове рањивости је висок јер би искоришћавањем такве рањивости нападач могао да добије приступ поверљивим подацима клијената, укључујући личне или осетљиве информације (табела 5). Један од најкритичнијих аспеката ове рањивости је могућност компромитовања података у историјским базама или у базама података у реалном времену. У случају манипулације подацима о стању опреме, нападач би могао да убаци погрешне информације које би резултирале да систем прикаже погрешан статус опреме, што може имати катастрофалне последице на рад и безбедност инфраструктуре. Такав сценарио може довести до прекида у раду, па чак и до физичког оштећења опреме.

Да би се ова рањивост умањила, предузете су следеће мере (слика 14):

- Имплементација јаке енкрипције за све податке у транзиту и у складишту.
- Континуирано проверавање интегритета података, као и коришћење механизама за проверу приступа базама података.
- Уведен је систем за надзор који прати и бележи неовлашћене покушаје приступа или измене података.
- Контролисани приступ базама података уз употребу ригорозних протокола за аутентификацију и ауторизацију обезбеђује да само овлашћене особе или системи могу приступити осетљивим подацима и радити са њима.
- Временски ограничен приступ осетљивим ресурсима (JIT) само када је то неопходно.
- Употреба RBAC модела ауторизације осигурава да сваки корисник и сервис имају само она права приступа која су им неопходна за обављање посла.
- Осетљиви подаци се чувају у трезору који има јаку аутентификацију, енкрипцију и аутоматизован процес ажурирања без људске интервенције.

Вероватноћа за експлоатацију ове рањивости је мала према табели 3 након примене предложених мера чак и ако је нападач инсајдер јер су комуникација и дискови кодирани и подаци заштићени од неовлашћеног приступа. Према матрици ризика представљеној у табели 7, ризик за ову рањивост је **низак**.

5.1.3 Одбацивање одговорности

Ако систему недостаје адекватно праћење активности, идентификација нападача који је извршио злонамерне операције постаје веома тежак задатак. Недостатак одговарајућих контрола, као што су вођење записа и њихов редовни преглед, не само да ограничава могућност откривања инцидента, већ и онемогућава атрибуцију унутар система. Уколико дође до искоришћавања ове рањивости, систем може остати рањив, а да администратори не буду свесни да ли је напад завршен или ће бити поновљен. Недостатак

информација о времену, природи и методама напада такође значи да је висок ризик од будућих напада, јер је тешко предвидети или припремити одбрану без детаљних информација о претходним инцидентима.

Међу најважнијим предузетим мерама (слика 14) је имплементација алата за стално праћење система, као што је SIEM. Ови алати омогућавају аутоматско прикупљање, анализу и корелацију података о догађајима из различитих делова инфраструктуре. SIEM поставља аутоматска правила за откривање и извештавање о сумњивим активностима или понашању система, што омогућава брзо реаговање у случају откривања неовлашћеног приступа. Овај систем игра кључну улогу у превенцији и раном откривању инцидената, као и у спречавању ескалације напада.

Имплементација вођења записа и надзора не само да омогућава идентификацију потенцијалних инцидената, већ такође дефинише скуп критичних догађаја који могу иницирати моментално обавештавање тима за безбедност у случају да дође до нарушавања безбедности. Поред тога, датотеке са евиденцијама су заштићене од неовлашћеног приступа и брисања, што осигурава да ниједан инсајдер неће моћи да избрише доказе или учини ове информације недоступним за анализу након инцидента. Ово је кључно за пост-инцидентну анализу и форензичко испитивање.

Сваки сервис унутар система има механизме за евиденцију релевантних активности, који не само да омогућавају праћење, већ и пружају јасну слику о томе ко је приступио одређеним ресурсима, шта је урађено и у којем тренутку. Ова евиденција је кључна за реаговање у случају безбедносног инцидента, јер омогућава тиму за безбедност да брзо анализира догађаје, идентификује рањивости и спречи поновно извршавање истог напада.

Иако је вероватноћа искоришћења ове рањивости веома мала, предузимање ових мера знатно смањује потенцијални ризик, чинећи да је систем боље припремљен за откривање и спречавање било каквих будућих напада. Према матрици ризика представљеној у табели 7, ризик за успешну злоупотребу ове рањивости је **веома низак**.

5.1.4 Откривање информација

Тајне представљају најосетљивију категорију информација и укључују податке као што су креденцијали за приступ систему, кључеви за енкрипцију, сертификати и друге поверљиве информације које омогућавају приступ критичним ресурсима. Њиховим компромитовањем нападач може добити директан приступ ресурсима и извршити неовлашћене операције, што би могло довести до озбиљних последица по безбедност система, као и до губитка поверења корисника и клијената. Поред тајни, систем садржи и поверљиве информације које су мање критичне, али и даље веома важне, као што су лични подаци потрошача. Цурење ових података може резултирати озбиљним правним последицама и високим новчаним казнама због кршења закона о заштити података, попут GDPR. То укључује информације које се налазе у бази података као што су имена, адресе, контакт подаци, као и финансијске информације. Информације од високог значаја за пословање, као што су подаци о стању опреме на терену, такође играју кључну улогу у раду система. Ови подаци се такође чувају у базама података и омогућавају администраторима и инжењерима да прате перформансе и статус критичних елемената система. У случају манипулације овим информацијама, могло би доћи до лажног представљања статуса опреме, што би довело до погрешних одлука и евентуалних

оштећења или прекида у раду. Изворни код, који садржи пословну логику система, такође је веома осетљив и његово откривање може довести до тога да нападачи открију како систем функционише, што би им омогућило да изведу прецизне нападе или саботажу. Компаније у великој мери зависе од заштите свог интелектуалног власништва, а крађа или измена изворног кода може озбиљно нарушити њихову конкурентност и репутацију. Утицај ове рањивости је веома висок јер би нападачи, стицањем приступа осетљивим информацијама, могли да изврше саботажу, изазову оперативне поремећаје и умање поверење клијената у сигурност и поузданост система.

Безбедносне мере предузете у циљу скривања ове рањивости укључују (слика 14):

- Имплементација одговарајућих механизама аутентификације и ауторизације, што осигурава да само овлашћени корисници могу приступити информацијама.

- Сегментација мреже ограничава комуникацију између микросервиса само на неопходне везе, чиме се смањује могућност да један компромитовани сервис угрози остале и открије осетљиве податке.

- Архитектура нултог поверења обезбеђује проверу permисија приликом сваког позива, небитно да ли он долази унутар или изван мреже.

- Сви подаци су енкриптовани како у транзиту тако и у мировању и заштићени моделом контроле приступа заснованим на улогама, што ограничава приступ само оним корисницима који имају дозволе за приступ одређеним ресурсима.

- Тајне као што су кључеви за енкриптовање и сертификати чувају се у посебном трезору, што додаје додатни слој заштите. Трезор не само да чува тајне, већ омогућава и редовну ротацију и управљање приступним подацима, чиме се смањује вероватноћа злоупотребе.

- Клијентске апликације које желе да приступе систему морају бити у одговарајућој мрежи и на "белој листи" која се редовно прати и контролише у реалном времену. Овај приступ осигурава да само проверене и одобрене апликације могу комуницирати са системом, смањујући ризик од неовлашћеног приступа.

- Вишефакторска аутентификација додаје додатни слој како би се осигурало да само овлашћени корисници могу приступити осетљивим информацијама.

- Спроводи се принцип минималних привилегија где се микросервисима дозвољава приступ само оним информацијама које су им неопходне за обављање задатака. Овај принцип минимизира изложеност осетљивих података и смањује ризик од њиховог откривања.

- Информације које више нису потребне се бришу.

Иако је вероватноћа за ову рањивост мала захваљујући снажним безбедносним мерама, ризик је и даље присутан, али се сматра **ниским** захваљујући свим предузетим корацима за заштиту осетљивих података и информација.

5.1.5 Ускраћивање услуге

Ако нападач покрене напад за дистрибуирано ускраћивање услуга, могао би озбиљно да угрози доступност сервиса или мреже, чинећи систем недоступним легитимним корисницима. Ова врста напада подразумева да велики број компромитованих уређаја истовремено шаље огроман број захтева према циљном систему, чиме се ствара ненормално велико оптерећење које инфраструктура не може да обради. Резултат овога је у крајњем случају гашење сервиса или значајно смањење њихове перформансе. У овом сценарију, корисници више нису у могућности да приступе кључним функцијама система. Поред саме недоступности услуге, један од додатних ризика у инфраструктурама рачунарског облака је повећано оптерећење система, што може довести до принудног вертикалног скалирања ресурса. Иако ово осигурава да систем остаје функционалан током напада, такав приступ може значајно повећати оперативне трошкове, посебно у рачунарском облаку где су ресурси динамички доступни, али по цени која расте са повећаним коришћењем. Велики број активних инстанци или додатних ресурса који су укључени током напада може довести до значајног финансијског губитка.

Утицај ове рањивости је висок јер, уколико је систем недоступан, компанија губи способност да комуницира са својим корисницима или опремом у пољу, што директно утиче на задовољство клијената и репутацију компаније. Поред тога, губитак пословних могућности током трајања прекида и потенцијални правни и регулаторни трошкови због неиспуњавања обавеза могу довести до озбиљних финансијских губитака. У случају да компанија мора да користи више ресурса него што је првобитно планирано, овај додатни трошак може значајно повећати укупне трошкове пословања.

Вероватноћа за ову рањивост се сматра ниском уколико се имплементирају следеће безбедносне мере (слика 14):

- Сви захтеви који долазе споља пролазе кроз улазни процесор, где се примењују алати платформе рачунарског облака који имају уграђене механизме заштите од DDoS напада. Ови алати су дизајнирани да идентификују и блокирају малициозне захтеве пре него што дођу до кључних ресурса, чиме се значајно смањује могућност преоптерећења система.

- Поред тога, SIEM алат активно прати и детектује сваки облик ненормалног понашања, како од стране спољашњих корисника, тако и од унутрашњих актера, укључујући кориснике у контролној соби и SCADA система. Уколико се открије да неки корисник или сервис изводи сумњиве активности, систем аутоматски реагује тако што се захтеви тог корисника више не обрађују, а он се уклања са беле листе дозвољених корисника.

- Подешавање ограничења броја захтева које један корисник или IP адреса може послати у одређеном временском периоду спречава DoS нападе и злоупотребе. Ово осигурава да злонамерни корисници не могу послати огромну количину захтева и преоптеретити систем.

- Коришћењем мрежне баријере дозвољена је комуникација која долази само са дефинисаних IP адреса.

- Проверава се и географска регија машине са које долази захтев и одбијају се сви захтеви који долазе из регија које нису релевантне за кориснике система.

Међутим, права рањивост у овом контексту није само малициозни корисник, већ и издржљивост система у суочавању са високим оптерећењем које може настати из других разлога. На пример, запослени могу ненамерно преоптеретити систем, чинећи га недоступним. Ово се може десити током управљања великим бројем операција које систем мора истовремено да обради. Слично томе, у случају невремена или природних катастрофа, када се дешавају значајне промене на терену у кратком временском периоду, систем може бити преплављен великим бројем захтева који одражавају реалне промене у статусу опреме на терену. У таквим ситуацијама, систем је дизајниран да одговори повећањем броја инстанци и ресурса како би се одржала функционалност и избегла потпуна недоступност. Ово аутоматско скалирање и распоређивање оптерећења је кључна мера за спречавање губитка услуге, али је истовремено важно да се обезбеди да систем не користи више ресурса него што је неопходно, како би се избегли непотребни трошкови.

Када се примене наведене мере, ризик од ове рањивости је **низак**. Систем има уграђене механизме, што осигурава да остане функционалан чак и у условима појачаних захтева или покушаја напада.

5.1.6 Елевација привилегија

У сценарију у којем нападач добија налог са ограниченим правима приступа, али успева да елевира своје привилегије до већих нивоа. Ова ескалација привилегија омогућава нападачу да приступи циљаним ресурсима и функционалностима које су иначе доступне само корисницима са већим привилегијама. Уколико нападач успе да добије веће привилегије, може изазвати озбиљне инциденте који доводе до прекида рада система, угрожавања његове безбедности и доступности. Нападач би могао да стекне увид у поверљиве информације о клијентима, укључујући личне податке или финансијске информације, што би угрозило приватност и безбедност тих клијената. Поред тога, елевација привилегија може омогућити нападачу да изврши саботажу на терену, као што је манипулација подацима или системима које теренске екипе користе за надзор и контролу инфраструктуре. У екстремним случајевима, нападач може имати капацитет да потпуно онеспособи критичне делове система, што би резултирало озбиљним пословним губицима физичких оштећења.

Вероватноћа да се ова рањивост искористи је веома мала захваљујући примени вишеструких безбедносних мера (слика 14):

- Сваки сервис у систему је заштићен контролом приступа заснованом на улогама, што значи да се привилегије корисника строго дефинишу и проверавају на нивоу сваког појединачног сервиса.

- Принцип минималних привилегија захтева да сваки корисник или микросервис има само она овлашћења која су неопходна за обављање његових задатака.

- Коришћењем OAuth2.0 и OIDC протокола за аутентификацију и ауторизацију имплементирана је делегација корисника чиме се онемогућава да корисник искористити неки микросервис као посредника како би извршио операције другог микросервиса за које нема пермисије.

- Од свих корисника се захтева да приликом пријаве на систем користе вишефакторску аутентификацију коју треба да понове пре него што приступе било којој критичној операцији. Овај додатни слој аутентификације чини знатно тежим за нападаче да искористе украдене креденцијале или да се представе као легитимни корисници.

- Листа корисника и корисничких група је доступна само администраторима система, што ограничава могућност нападача да манипулише тим подацима. Свака промена у пермисијама корисника или група, укључујући промоцију корисника са мањим правима на више нивое привилегија, захтева од администратора понављање вишефакторске аутентификације. Ова мера обезбеђује да се неовлашћене промене у системским привилегијама не могу извршити без одобрења овлашћеног лица.

- Ниједан кориснички налог, укључујући администраторски, не сме имати највише привилегије као подразумеване. Уместо тога, неопходно је користити алат који омогућава привремено повећање привилегија за одређени временски период, током којег се извршавају радње које захтевају виши ниво приступа. Приликом подношења захтева за повећање привилегија, корисник мора навести разлог за приступ, након чега се разматра и одобрава или одбија тај захтев.

- Сваки покушај елевирања привилегија је забележен у системима за надзор. Редовно праћење записа омогућава брзо откривање покушаја неовлашћеног приступа.

- Раздвајање одговорности између тимова за развој, тестирање и продукцију осигурава да ниједна особа или тим нема превелике привилегије у целом систему.

Због ових ригорозних мера, ризик од искоришћавања ове рањивости сматра се **ниским**. Иако потенцијални утицај може бити веома висок у случају успешне елевације привилегија, напредни безбедносни механизми и политике контроле приступа осигуравају да су такви инциденти изузетно ретки и тешко изводљиви.

5.2 Резултат анализе

У табели испод је приказан сумиран преглед резултата STRIDE анализе, у којој је систем посматран као целина.

Рањивост	Утицај	Вероватноћа	Ризик
Лажирање	Веома висок	Ниска	Низак
Неовлашћено мењање	Висок	Ниска	Низак
Одбацивање одговорности	Веома низак	Веома ниска	Веома низак
Откривање информација	Висок	Ниска	Низак
Ускраћивање сервиса	Висок	Ниска	Низак
Елевација привилегија	Висок	Веома ниска	Низак

Табела 8 - Сумиран приказ STRIDE анализе

Ова анализа је коришћена да се идентификују потенцијалне рањивости у шест категорија: лажирање идентитета (S), неовлашћене измене података (T), одбацивање одговорности (R), откривање информација (I), ускраћивање сервиса (D) и елевација привилегија (E). Свака од идентификованих рањивости је процењена на основу могућности искоришћења и њеног потенцијалног утицаја на систем. Резултати указују на то да је ризик од свих наведених рањивости низак или веома низак, што потврђује да је предложена архитектура система дизајнирана на начин који обезбеђује висок ниво безбедности. Додатно, пажљивим планирањем мера заштите и редовним праћењем сигурносних параметара, систем ће моћи да одржи овај ниво заштите и одбрани се од могућих будућих напада. Претходно наведено показује да је доказана следећа хипотеза:

STRIDE методологија за анализу ризика је применљива и у контексту развоја модерних индустријских контролних система са микросервисном архитектуром.

6. ЗАКЉУЧАК

Критичне инфраструктуре (КИ) морају бити у складу са најстрожијим безбедносним регулативама и стандардима где одржавање усклађености са стандардима представља посебан изазов. Једна од главних препрека за премештање КИ система у рачунарски облак била је управо бојазан у погледу безбедности. Коришћење архитектуре засноване на микросервисима уводи вишеструке предности у погледу перформанси ОТ система. Поред тога, приликом постављања таквог система у рачунарски облак, снижавају се почетни трошкови улагања и одржавања.

Циљ овог истраживања био је да се анализира архитектура заснована на микросервисима за ОТ системе са безбедносне тачке гледишта и да се предложи стратегија ублажавања која ће смањити вероватноћу искоришћавања нађених рањивости. Током истраживања се дошло до закључка да принцип нултог поверења треба да буде уграђен у архитектуру система још у фази пројектовања. Следећи кораци су спроведени како би се дефинисала безбедна архитектура референтног система:

1. Изабрана је референтна архитектура ИКС заснована на микросервисној архитектури у рачунарском облаку
2. Систем, његове компоненте и ток података између њих су анализирани.
3. После анализе литературе дијаграм рањивости је креиран за референтну архитектуру система.
4. Рањивости су анализиране и груписане.
5. За сваку рањивост одређена је мера чијом се применом смањује могућност њеног експлоатисања.
6. Предложена је измена архитектуре система узимајући у обзир предложене мере.
7. Као тест безбедности архитектуре, извршена је STRIDE анализа по компонентама и процењен ризик за сваку рањивост.

Као први корак у анализи архитектуре, сервиси су подељени у три групе: основни, периметарски и јавни сервиси. Урађена је сегментација мреже при чему свака група сервиса има своју, одвојену мрежу, при чему су дефинисана улазна и излазна правила и све поруке енкриптоване и потписане. Комуникација са клијентском апликацијом и SCADA системом иде кроз енкриптовани VPN тунел и мрежну баријеру. Јавним сервисима могу да приступе и уређаји споља, где сва комуникација пролази кроз улазни процесор који се састоји из четири компоненте у рачунарском облаку, осигуравајући безбедну комуникацију. Очување интегритета података је јако важна као и правовремено откривање и реакција на покушаје промене података. Како ови системи често рукују са осетљивим подацима о личности, мора се осигурати правилно руковање, складиштење и

пренос тих података. Криптографија, заштита од пресретања података и сигурни протоколи комуникације су од суштинског значаја. За складиштење осетљивих података, као што су кључеви за енкриптовање или сертификати, користи се трезор. Правилна аутентификација и ауторизација корисника, уређаја и сервиса је обавезна да би се спречио неовлашћен приступ. У ту сврху се користи провајдер идентитета и протоколи OAuth2.0 и OIDC. Строга контрола приступа заснована на улогама у складу са принципима одбране у дубину и принципа најмање привилегије и управљање привилегијама мора бити имплементирано. Корисницима, уређајима и сервисима треба давати само оне привилегије које су им потребне за обављање посла. Анонимни приступ систему је забрањен, јака лозинка и вишефакторска аутентификација су обавезни за све кориснике. За аутентификацију микросервиса користе се сертификати. Архитектура је у складу са препорукама принципа нултог поверења. Евидентирање и праћење активности се спроводи од стране различитих алата који су доступни у инфраструктури рачунарског облака. Одговарајућа упозорења и аларми се генеришу у случају ненормалног понашања система како би се повећала вероватноћа раног откривања напада. Физичка сигурност опреме, хардвера и инфраструктуре је такође битна и она је у надлежности пружаоца услуга у рачунарском облаку.

STRIDE методологија је коришћена за анализу горе описане референтне архитектуре ИКС. Анализа ризика на нивоу сервиса показала је да је вероватноћа експлоатације претњи значајно смањена имплементацијом предложених мера па је самим тим и ризик низак.

Што се тиче правца даљег истраживања у овој области, неопходно је извршити свеобухватно тестирање безбедности предложене архитектуре. Ово укључује спровођење тестова пенетрације, анализу отпорности на мрежне нападе, и верификацију сигурности корисничких података у складу са актуелним стандардима. Поред тога, потребно је детаљно анализирати предложене мере са аспекта цене развоја, узимајући у обзир трошкове имплементације, одржавања и потенцијалних побољшања система. Ова анализа може помоћи да се утврди уравнотеженост између постизања високог нивоа безбедности и оптимизације ресурса, као и да се процени утицај на укупни буџет. Такође је битна анализа перформанси система након имплементације свих предложених безбедносних мера. Потребно је потврдити да предузете мере не утичу на деградирање одзива система.

ЛИТЕРАТУРА

[1] *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and Designation of European Critical Infrastructures and the assessment of the need to improve their protection.* На мрежи: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF [Последњи приступ Јун 2024].

[2] *Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services.* На мрежи: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202302450 [Последњи приступ Јун 2024].

[3] *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* На мрежи: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive [Последњи приступ Јун 2024].

[4] Critical Infrastructure Protection: "*National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*", United States Government Accountability Office, GAO-23-105468, 2023.

[5] Cybersecurity: "*Interior Needs to Address Threats to Federal Systems and Critical Infrastructure*", United States Government Accountability Office, GAO-23-106869, 2023.

[6] Alcaraz, C. and Zeadally, S. "*Critical control system protection in the 21st century*". Computer 46, no. 10, pp. 74-83, 2013.

[7] *Critical infrastructure resilience at EU-level*. На мрежи: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-

radicalisation/protection/critical-infrastructure-resilience_en#related-links [Последњи приступ Јун 2024].

[8] Asghar, Muhammad Rizwan, Qinwen Hu, and Sherali Zeadally. "*Cybersecurity in industrial control systems: Issues, technologies, and challenges.*" Computer Networks 165, p. 106946, 2019.

[9] S. Stoja, S. Vukmirovic, N. Dalcekovic, D. Capko and B. Jelacic, "*Accelerating Performance in Critical Topology Analysis of Distribution Management System Process by Switching from Monolithic to Microservices*", Revue Roumaine des Sciences Techniques Serie Electrotechnique et Energetique 63, no. 3, pp. 338-343, 2018.

[10] Berardi, Davide, Saverio Giallorenzo, Jacopo Mauro, Andrea Melis, Fabrizio Montesi, and Marco Prandini. "*Microservice security: a systematic literature review*." PeerJ Computer Science 8, p. e779, 2022.

[11] Zhou, Chunjie, Bowen Hu, Yang Shi, Yu-Chu Tian, Xuan Li, and Yue Zhao. "*A unified architectural approach for cyberattack-resilient industrial control systems.*" Proceedings of the IEEE 109, no. 4, pp. 517-541, 2020.

[12] *World's Critical Infrastructure Suffered 13 Cyber Attacks Every Second in 2023*. На мрежи: https://securitytoday.com/Articles/2024/01/29/World-Critical-Infrastructure-Suffered-13-Cyber-Attacks-Every-Second-in-2023.aspx. [Последњи приступ Јун 2024].

[13] Pattanayak, Animesh, and Matt Kirkland. "*Current cyber security challenges in ICS*." In 2018 IEEE International Conference on Industrial Internet (ICII), pp. 202-207, 2018.

[14] K. Hemsley and R. Fisher, „*A history of cyber incidents and threats involving industrial control systems.*" Critical Infrastructure Protection XII: 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, March 12-14, 2018, Revised Selected Papers 12, Springer, pp. 215-242, 2018.

[15] T. Miller, A. Staves, S. Maesschalck, M. Sturdee and B. Green, „*Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems*." International Journal of Critical Infrastructure Protection 35, p. 100464, 2021.

[16] M. Baezner and P. Robin, „*Stuxnet*“ ETH Zurich, 2017.

[17] D. Kushner „*The real story of Stuxnet*.“ Ieee Spectrum 50, no. 3, pp. 48-53, 2013.

[18] *H2 2023 – a brief overview of main incidents in industrial cybersecurity*. На мрежи: https://ics-cert.kaspersky.com/publications/reports/2024/04/11/h2-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/ [Poslednji pristup April 2024].

[19] Bouramdane, Ayat-Allah. "*Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process*." Journal of Cybersecurity and Privacy 3, no. 4, pp. 662-705, 2023.

[20] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan and N. Meskin, "*Cybersecurity for Industrial Control Systems: A survey*", Computers & security 89, p.101677, 2020.

[21] Aslam, Muhammad Muzamil, Ali Tufail, Rosyzie Anna Awg Haji Mohd Apong, Liyanage Chandratilak De Silva, and Muhammad Taqi Raza. "*Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective*." IEEE Access, 2024.

[22] Fovino, Igor Nai, Luca Guidi, Marcelo Masera, and Alberto Stefanini. "*Cyber security assessment of a power plant.*" Electric Power Systems Research 81, no. 2, pp. 518-526, 2011.

[23] Alcaraz, Cristina, and Sherali Zeadally. "*Critical infrastructure protection: Requirements and challenges for the 21st century.*" International journal of critical infrastructure protection 8, pp. 53-66, 2015.

[24] Z. M. Yusop and J. H. Abawajy, “*Analysis of insiders attack mitigation strategies*”, Procedia-Social and Behavioral Sciences, no. 129, pp. 581-591, 2014

[25] Saxena, Neetesh, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap, “*Impact and key challenges of insider threats on organizations and critical businesses*”, Electronics 9, no. 9, pp. 1460, 2020, 2020.

[26] Nurse, Jason RC, Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon RT Wright, and Monica Whitty, "*Understanding insider threat: A framework for characterising attacks*", 2014 IEEE security and privacy workshops, pp. 214-228. IEEE, 2014.

[27] Kim, Aram, Junhyoung Oh, Jinho Ryu, and Kyungho Lee, "*A review of insider threat detection approaches with IoT perspective*", IEEE Access 8, pp. 78847-78867, 2020.

[28] Agrafiotis, Ioannis, Jason RC Nurse, Oliver Buckley, Phil Legg, Sadie Creese, and Michael Goldsmith, "*Identifying attack patterns for insider threat detection*", Computer Fraud & Security 2015, no. 7, pp. 9-17, 2015.

[29] Stanojevic, Marina, Darko Capko, Imre Lendak, Sebastijan Stoja, and Bojan Jelacic. "*Fighting Insider Threats, with Zero-Trust in Microservice-based, Smart Grid OT Systems*." Acta Polytechnica Hungarica, vol. 20, no. 6, pp. 229-248, 2023.

[30] *The Cyber Kill Chain.* На мрежи: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Последњи приступ Јун 2024].

[31] Ani, Uchenna P. Daniel, Hongmei He, and Ashutosh Tiwari. "*Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective*." Journal of Cyber Security Technology 1, no. 1, pp. 32-74, 2017.

[32] Islam, Shama Naz, Zubair Baig, and Sherali Zeadally. "*Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures*." IEEE Transactions on Industrial Informatics 15, no. 12, pp. 6522-6530, 2019.

[33] A. Pereira-Vale, E. B. Fernandez, R. Monge, H. Astudillo and G. Márquez, "*Security in microservice-based systems: A Multivocal literature review*", Computers & Security 103, p.102200, 2021.

[34] N. Mateus-Coelho, M. Cruz-Cunha and L. Gonzaga Ferreira, "*Security in Microservices Architectures, Procedia Computer Science*", Procedia Computer Science 181, pp. 1225-1236, 2021.

[35] Pereira-Vale A, Márquez G, Astudillo H and Fernandez EB, "*Security Mechanisms Used in Microservices-based Systems: A Systematic Mapping*", XLV Latin American Computing Conference (CLEI). IEEE, p. 01–10, 2019.

[36] Flora, José, "*Improving the security of microservice systems by detecting and tolerating intrusions*", IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 131-134, 2020.

[37] de Almeida, Murilo Góes, and Edna Dias Canedo, "*Authentication and Authorization in Microservices Architecture: A Systematic Literature Review*", Applied Sciences 12, no. 6, p. 3023, 2022.

[38] T. Yarygina and A. H. Bagge, "*Overcoming Security Challenges in Microservice Architectures*", IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 11-20, 2018.

[39] Baker, Oras, and Quy Nguyen. "*A novel approach to secure microservice architecture from owasp vulnerabilities.*" CITRENZ Conference 2019. 2019.

[40] Chen, Dong, Guiran Chang, Lizhong Jin, Xiaodong Ren, Jiajia Li, and Fengyun Li. "*A novel secure architecture for the internet of things*." IEEE Fifth International Conference on Genetic and Evolutionary Computing, pp. 311-314, 2011.

[41] Hannousse, Abdelhakim, and Salima Yahiouche. "*Securing microservices and microservice architectures: A systematic mapping study*." Computer Science Review 41, p. 100415, 2021.

[42] Rudrabhatla, Chaitanya K. "*Security design patterns in distributed microservice architecture.*" IJCSIS 18 No. 7, p. 03395, 2020.

[43] Ahmadvand, Mohsen, Alexander Pretschner, Keith Ball, and Daniel Eyring, "*Integrity protection against insiders in microservice-based infrastructures: From threats to a security framework*", Federation of International Conferences on Software Technologies: Applications and Foundations, pp. 573-588. Springer, Cham, 2018.

[44] Aksakalli, Işıl Karabey, Turgay Çelik, Ahmet Burak Can, and Bedir Tekinerdoğan. "*Deployment and communication patterns in microservice architectures: A systematic literature review*." Journal of Systems and Software 180, p. 111014, 2021.

[45] Yussupov, Vladimir, Uwe Breitenbücher, Christoph Krieger, Frank Leymann, Jacopo Soldani, and Michael Wurster. "*Pattern-based modelling, integration, and deployment of microservice architectures*." IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC), pp. 40-50, 2020.

[46] Abdelfattah, Amr S., and Tomas Cerny. "*Roadmap to reasoning in microservice systems: a rapid review.*" Applied Sciences 13, no. 3, p. 1838, 2023.

[47] Singh, Vindeep, and Sateesh K. Peddoju. "*Container-based microservice architecture for cloud applications.*" In 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 847-852, 2017.

[48] Y. Sun, S. Nanda, and T. Jaeger, "*Security-as-a-service for microservices-based cloud applications*", 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 50-57, 2015.

[49] Buck, Christoph, Christian Olenberger, André Schweizer, Fabiane Völter, and Torsten Eymann, "*Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust*", Computers & Security 110, p. 102436, 2021

[50] Prakash, Chandra. "*Zero-Trust Architecture Approach to Secure Microservices for the Healthcare Insurance Industry.*" PhD diss., University of the Cumberlands, 2024.

[51] Dongiovanni, Alessio. "*Zero Trust Network Security Model in Containerized Environments.*" PhD diss., Politecnico di Torino, 2024.

[52] de Weever, Catherine, and Marios Andreou, "*Zero trust network security model in containerized environments*", University of Amsterdam, The Netherlands, 2020.

[53] S. Rodigari, D. O'Shea, P. McCarthy, M. McCarry and S. McSweeney, "*Performance Analysis of Zero-Trust multi-cloud*", 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), pp. 730-732, 2021.

[54] I. Ahmed, T. Nahar, S. Sultana Urmi and K. Abu Taher, "*Protection of sensitive data in zero trust model*", Proceedings of the International Conference on Computing Advancements, pp. 1-5, 2020.

[55] Mehraj, Saima, and M. Tariq Banday, "*Establishing a zero trust strategy in cloud computing environment*", 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, 2020.

[56] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "*Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust*", Computers & Security 110, p. 102436, 2021.

[57] Nina, Hernan, José Antonio Pow-Sang, and Mónica Villavicencio. "*Systematic mapping of the literature on secure software development.*" IEEE Access 9, pp. 36852-36867, 2021.

[58] Malatji, Masike, Annlizé L. Marnewick, and Suné Von Solms. "*Cybersecurity capabilities for critical infrastructure resilience.*" Information & Computer Security 30, no. 2, pp. 255-279, 2022.

[59] Syafrizal, Melwin, Siti R. Selamat, and Nurul A. Zakaria. "*Analysis of cybersecurity standard and framework components.*" International Journal of Communication Networks and Information Security 12, no. 3, p. 417-432, 2020.

[60] IEC 62443, *Security of Industrial Automation and Control Systems*. На мрежи: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf. [Последњи приступ Јун 2024].

[61] ISO 27000, *Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabular*. International Organization for Standardization ISO, Geneve, 2009.

[62] ISO 27001, *Information Technology, Security Techniques, Information Security Management Systems, Requirements*. International Organization for Standardization

ISO, Geneve, 2005. [На мрежи]. Available: https://iso.org.rs/iso-27001/. [Последњи приступ Јун 2024].

[63] ISO 27017, *Code of Practice for Information Security Controls Based on Iso/Iec 27002 for Cloud Services*. International Organization for Standardization ISO. 2015.

[64] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. На мрежи: https://www.iso.org/standard/76559.html [Последњи приступ Јун 2024].

[65] *NERC CIP Reliability Standards.* На мрежи: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx. [Последњи приступ Јун 2024].

[66] *Security Guideline for the Electricity Sector - Supply Chain.* На мрежи: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf [Последњи приступ Јун 2024].

[67] *SOC 2 - SOC for Service Organizations: Trust Services Criteria*. На мрежи: https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2 [Последњи приступ Јун 2024].

[68] *SOC 2 Compliance*. На мрежи: https://www.imperva.com/learn/data-security/soc-2-compliance/ [Последњи приступ Јун 2024].

[69] Pascoe, Cherilyn, Stephen Quinn, and Karen Scarfone. "*The NIST Cybersecurity Framework (CSF) 2.0.*", 2024.

[70] Souppaya, M. , Morello, J. and Scarfone and K. "*Application Container Security Guide",* Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-190, 2017.

[71] Stouffer, K. , Pease, M. , Tang, C. , Zimmerman, T. , Pillitteri, V. , Lightman, S. , Hahn, A. , Saravia , S. , Sherule, A. and Thompson, M. "*Guide to Operational Technology (OT) Security*", Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-82r3, 2023.

[72] National Institute of Standards and Technology, "*NIST Cloud Computing Security Reference Architecture*.", 2013.

[73] Liu, F. , Tong, J. , Mao, J. , Bohn, R. , Messina, J. , Badger, M. and Leaf, D. "*NIST Cloud Computing Reference Architecture*", Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.500-292, 2011.

[74] Jansen, W. and Grance, T. "*Guidelines on Security and Privacy in Public Cloud Computing*", Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-144, 2011

[75] Grance, T. and Mell, P. "*The NIST Definition of Cloud Computing*", Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.SP.800-145, 2011

[76] *Securing key infrastructures across the Union.* На мрежи: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services [Последњи приступ Јун 2024].

[77] *OWASP Top Ten*. На мрежи: https://owasp.org/www-project-top-ten/ [Последњи приступ Јун 2024].

[78] *CWE TOP 25 Most Dangerous Software Errors*. На мрежи: https://www.sans.org/top25-software-errors/ [Последњи приступ Јун 2024].

[79] *Cloud Controls Matrix (CCM).* На мрежи: https://cloudsecurityalliance.org/research/cloud-controls-matrix [Последњи приступ Јун 2024].

[80] *CSA Consensus Assessments Initiative Questionnaire (CAIQ).* На мрежи: https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf [Последњи приступ Јун 2024].

[81] *CIS Benchmarks List.* На мрежи: https://www.cisecurity.org/cis-benchmarks [Последњи приступ Јун 2024].

[82] *General Data Protection Regulation*. На мрежи: https://gdpr-info.eu/ [Последњи приступ Јун 2024].

[83] Stafford, V. A. "*Zero trust architecture*." NIST special publication 800, p.207, 2020.

[84] Бојан Јелачић, "*Методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима*", Докторска дисертација, Нови Сад, 2022.

[85] B.Zhu, A.Joseph and S.Sastry, "*A taxonomy of cyber attacks on SCADA systems*" Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing, pp. 380–388, 2011.

[86] Jelacic, Bojan, Imre Lendak, Sebastijan Stoja, Marina Stanojevic, and Daniela Rosic. "*Security risk assessment-based cloud migration methodology for smart grid OT services*." Acta Polytechnica Hungarica 17, no. 5, pp. 113-134, 2020.

[87] Leszczyna, Rafal, Igor Nai Fovino, and Marcelo Masera. "*Approach to security assessment of critical infrastructures' information systems.*" IET Information Security 5, no. 3, pp. 135-144, 2011.

[88] Leszczyna, R., Fovino, I.N., Masera, M.: "*Simulating Malware with MAlSim*", J. Comput. Virol. 6, pp. 65–75, 2008.

[89] J.-M. Flaus, "*Components of an industrial control system*", Wiley Data and Cybersecurity, 2019.

[90] IEC 62443-3-3 "*Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*.", Geneva, Switzerland, 2013.

[91] *Microsoft MSDN documentation, the Threat Modeling tool*. На мрежи: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-mitigations

[92] Homeland Security "*Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies."* Industrial Control Systems Cyber Emergency Response Team. September 2016. www.iiconsortium.org.

[93] Abdelghani, Tschroub. "*Implementation of defense in depth strategy to secure industrial control system in critical infrastructures*." American Journal of Artificial Intelligence 3, no. 2, pp. 17-22, 2019.

[94] Malatji, Masike. "*Industrial control systems cybersecurity: Back to basic cyber hygiene practices*." International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1-7, 2022.

[95] Jadidi, Zahra, Shantanu Pal, Qinyi Li, and Ernest Foo. "*Cyber Security Resilience in Industrial Control Systems using Defence-in-Depth and Zero Trust*." 16th International Conference on Sensing Technology (ICST), pp. 1-6, 2023.

[96] *Microsoft MSDN documentation, the STRIDE Threat Model*. На мрежи: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[97] Khalil, Shaymaa Mamdouh, Hayretdin Bahsi, and Tarmo Korõtko. "*Threat modeling of industrial control systems: A systematic literature review*." Computers & Security, p. 103543, 2023.

[98] Möller, Dietmar PF "*NIST cybersecurity framework and MITRE cybersecurity criteria*." Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, pp. 231-271. Cham: Springer Nature Switzerland, 2023.

[99] Dias, Wajjakkara Kankanamge Anthony Nuwan, and Prabath Siriwardena. "*Microservices security in action*." Simon and Schuster, 2020.

[100] Hardt, D., Ed., "*The OAuth 2.0 Authorization Framework*", RFC 6749, DOI 10.17487/RFC6749, October 2012. На мрежи: https://www.rfc-editor.org/info/rfc6749.

[101] Sakimura, N., Ed., Bradley, J., and N. Agarwal, "*Proof Key for Code Exchange by OAuth Public Clients*", RFC 7636, DOI 10.17487/RFC7636, September 2015. На мрежи: https://www.rfc-editor.org/info/rfc7636

[102] Campbell, B., Bradley, J., Sakimura, N., and T. Lodderstedt, "*OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens*", RFC 8705, DOI 10.17487/RFC8705, February 2020. На мрежи: https://www.rfc-editor.org/info/rfc8705

БИОГРАФИЈА

Марина Станојевић је рођена 25.6.1992. у Новом Саду. Завршила је основну школу "Прва војвођанска бригада" у Новом Саду, након чега је уписала гимназију "Јован Јовановић Змај", смер обдарени ученици у математичкој гимназији. Након завршене средње школе, Марина је уписала основне студије на Факултету техничких наука, смер Рачунарство и аутоматика. Основне студије завршава 2015. просеком 9.92, мастер студије 2016. просеком 10 након чега уписује докторске студије на студијском програму Енергетика, електроника и телекомуникације.

Своју каријеру је започела у индустрији 2016. у компанији Schneider Electric где је почела као развојни инжењер, а од октобра 2023. промовисана на позицију софтверског архитекте где се и данас налази. Марина ради у тиму који је задужен за миграцију система критичне инфраструктуре у рачунарски облак. Рад у овом пољу јој је омогућио да се упозна са реалним безбедносним изазовима на које наилази индустријски сектор. Марина је упоредо са радом у индустрији била ангажована и као асистент на Факултету техничких година у периоду од 2016. – 2023. Кроз рад са студентима на предметима Индустријски комуникациони протоколи и Cloud Computing учествовала је у разним пројектима и напредовала у улози предавача.

Марина је положила све испите предвиђене планом и програмом докторских студија. Коаутор је и аутор на више научних радова који су објављени у међународним часописима и конференцијама.

БИБЛИОГРАФИЈА

1. МАРИНА СТАНОЈЕВИЋ, -, СЕРВИС ЗА УПРАВЉАЊЕ КВАРОМ У ЕЛЕКТРОДИСТРИБУТИВНИМ МРЕЖАМА, ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА, НОВИ САД, -1, VOL. -, NO. 11, PP. 2035 - 2038, ISSN: 0350-428X, UDC: -, DOI: -5035062-, 2016.
2. С. ДЕЈАНОВИЋ, Ј. СТАНКОВСКИ, М. СТАНОЈЕВИЋ, И. ЛЕНДАК, COST-BENEFIT ANALYSIS OF MIGRATING THE ADMS TO THE COMPUTING CLOUD, COST-BENEFIT ANALYSIS OF MIGRATING THE ADMS TO THE COMPUTING CLOUD, ICIST 2017 - 7TH INTERNATIONAL CONFERENCE ON INFORMATION SOCIETY AND TECHNOLOGY, VOL. 1, PP. 90 - 92, ISBN: 978-86-85525-19-3, KOPAONIK, SERBIA, 12. - 15. MAR, 2017
3. Б. ЈЕЛАЧИЋ, Д. РОСИЋ, И. ЛЕНДАК, М. СТАНОЈЕВИЋ, С. СТОЈА, STRIDE TO A SECURE SMART GRID IN A HYBRID CLOUD, INDUSTRIAL CONTROL SYSTEMS & OF CYBER-PHYSICAL SYSTEMS CYBERICPS, ESORICS 2017, PP. 77 - 90, ISBN: 978-3-319-72817-9, OSLO, 11. - 15. SEP, 2017
4. N. STOJAKOVIĆ, M. STANOJEVIĆ, D. ČAPKO, T. GRBIĆ, INCIDENT SIMULATOR FOR ADMS PERFORMANCE TESTING, PROCEEDINGS OF PAPERS – 6TH INTERNATIONAL CONFERENCE ON ELECTRICAL, ELECTRONIC AND COMPUTING ENGINEERING, ICETRAN 2019, DRUŠTVO ZA ETRAN, BEOGRAD I AKADEMSKA MISAO, BEOGRAD , PP. 170 - 173, ISBN: 978-86-7466-785-9, SREBRNO JEZERO, 3. - 6. JUN, 2019
5. Н. ПОПОВИЋ, М. СТАНОЈЕВИЋ, И. ШЕШКАР, AN OPTIMAL PLACEMENT OF ADMS IN CLOUD DATA CENTER, AN OPTIMAL PLACEMENT OF ADMS IN CLOUD DATA CENTER, IEEE EUROCON 2019 -18TH INTERNATIONAL CONFERENCE ON SMART TECHNOLOGIES, ISBN: 978-1-5386-9301-8, НОВИ САД, 1. - 4. JUL, 2019
6. Б. ЈЕЛАЧИЋ, И. ЛЕНДАК, С. СТОЈА, М. СТАНОЈЕВИЋ, Д. РОСИЋ, SECURITY RISK ASSESSMENT-BASED CLOUD MIGRATION METHODOLOGY FOR SMART GRID OT SERVICES, ACTA POLYTECHNICA HUNGARICA, VOL. 17, NO. 5, PP. 113-134, 2020.
7. М.СТАНОЈЕВИЋ, Д. ЧАПКО, И. ЛЕНДАК, С. СТОЈА, Б. ЈЕЛАЧИЋ, FIGHTING INSIDER THREATS, WITH ZERO-TRUST IN MICROSERVICE-BASED, SMART GRID OT SYSTEMS, ACTA POLYTECHNICA HUNGARICA, VOL. 20, NO. 6, PP. 229-248, 2023

ДОДАТАК А – КЉУЧНЕ БЕЗБЕДНОСНЕ ОСНОВЕ

Ниво безбедности није само техничка, већ и економска одлука и зависи од система и делатности у којој се користи. У наставку су наведене мере које су основа за безбедан систем [99]:

1. ***Аутентификација штити систем од лажирања***. Аутентификација је процес идентификације захтевајуће стране са циљем заштите система од лажирања. Захтевајућа страна може бити сервис или корисник. За аутентификацију корисника може се захтевати корисничко име и лозинка са вишефакторском аутентификацијом. Најпопуларнији облик вишефакторске аутентификације је једнократна лозинка послата путем поруке на мобилни телефон, а користе се и јачи облици који укључују биометрију, сертификате и брзу идентификацију на мрежи (енг. FIDO). Са друге стране, за аутентификацију сервиса опције су сертификати и токени (JWT).

2. ***Интегритет штити систем од неовлашћеног приступа подацима.*** Приликом преноса података од клијентске апликације до микросервиса или од једног микросервиса до другог, нападач може да пресретне комуникацију и да промени податке. Како би се системи заштитили од ове врсте напада, потребно је увести одређене мере које ће обезбедити примаоцу да открије да је порука измењена и да такав захтев одбаци. Најчешћи начин заштите интегритета поруке је потписивање. Коришћење комуникационих канала који су заштићени транспортним слојем безбедности гарантује одржање интегритета порука. Уколико се за комуникацију између микросервиса користи HTTPS, интегритет размењених порука је заштићен док су у транзиту. Поред транзита, интегритет података мора бити заштићен и у складишту. Нападач који приступи систему може да покуша да измени запис како би избрисао све доказе, тако да је потребно имплементирати контролу приступа над записима. Један начин за обезбеђивање интегритета записа је периодично израчунавање кратких, фиксних бројева који представљају сажетке записа, њихово енкриптовање и безбедно чување.

3. ***Неопозивост – оно што се уради једном остаје заувек***. Неопозивост је важан аспект информационе безбедности који спречава негирање било чега што је урађено или уговорено. У дигиталном свету, користи се дигитални потпис да се постигне неопозивост. Мора се обезбедити да се трансакције уписују заједно са временским ознакама и потписом као и да се ти записи чувају дужи временски период. Ово је важно јер у случају да иницијатор касније покуша да оспори трансакцију постоји запис који доказује да се трансакција догодила.

4. ***Поверљивост штити од ненамерног откривања информација***. Нападач може пресрести комуникацију и преузети податке или добити приступ складишту података или резервним копијама података. Криптографска операција се брине да кодирани подаци буду видљиви само намењеном примаоцу. Већина система за управљање базама података пружа функције за аутоматско кодирање, доступно је и кодирање на нивоу диска. Кодирање у апликативном коду је још једна опција, при чему сама апликација кодира податке пре него што их пошаље или складишти. Код избора методе енкрипције битно је наћи оптимално решење јер је енкрипција операција која захтева много ресурса и која има значајан утицај на перформансе система.

5. ***Доступност – одржавање система у функцији***. Иако има кључну улогу, није само дизајн безбедности система нешто о чему треба бринути да би се одржао систем у функцији. Грешка у функционалности апликације може угрозити функционисање система. За разлику од монолитних апликација, у микросервисима, цео систем неће пасти ако постоји грешка у једној компоненти или микросервису. Архитектура безбедности са више слојева омогућава да сваки слој буде дизајниран тако да се брине о различитим типовима напада и тиме да се нападач одбије на највишем слоју. На пример, заштита од DoS/DDoS напада је најбоље да буде на мрежном слоју. Једна од опција је мрежна баријера који је на ивици мреже и може да блокира злонамерне кориснике. Међутим у случају DDoS напада, мрежна баријера није довољна, већ је потребно имплементирати решења која нуде специјализовани продавци (енг. *vendors*). На нивоу апликације, најбоље што се може урадити је одбијање захтева чим је утврђено да није валидан.

6. ***Ауторизација***. Аутентификација даје информације о кориснику или захтевајућој страни. Ауторизација проверава да ли аутентификовани корисник има довољна права да изврши тражену операцију на систему. У типичној микросервисној архитектури, ауторизација може да се ради на улазној тачки или на нивоу сваког микросервиса.

ДОДАТАК Б – ИЗАЗОВИ МИКРОСЕРВИСНЕ АРХИТЕКТУРЕ

У наставку су побројани главни изазови у безбедности микросервиса [99]:

1. ***Већа површина напада*** – у поређењу са монолитним апликацијама које су имале неколико улазних тачака, микросервисна архитектура има много већи број улазних тачака. Ово резултује већом површином напада и то је један од основних изазова у изградњи безбедне архитектуре за микросервисе. Свака улазна тачка микросервиса мора бити заштићена истим механизмима. Безбедност система је јака колико и безбедност њене најслабије компоненте.
2. ***Лошије перформансе због дистрибуираних безбедносних тестирања*** – за разлику од монолитне апликације, сваки микросервис мора спроводити независно испитивање безбедности. Валидација захтева може да захтева повезивање са неким удаљеним приступним сервисом. Ове понављајуће, дистрибуиране безбедносне провере могу значајно допринети кашњењу и утицати на деградирање перформанси система. Неки ово избегавају тако што једноставно верују мрежи и не спроводе сигурносне провере на сваком микросервису. Међутим, веровање мрежи постало је антиобразац, и индустрија се креће ка принципу нултог поверења, поготово за критичне инфраструктуре. Принцип нултог поверења, захтева да се безбедносне мере имплементирају ближе ресурсу у мрежи. Сваки безбедни дизајн микросервиса мора узети у обзир перформансе и предузети мере предострожности како би се адресирали евентуални недостаци.
3. ***Сложена поставка система*** – поставке система великог обима, са хиљадама микросервиса, постали су реалност. Управљање овим поставкама би било изузетно изазовно и склоно грешкама без аутоматизације. Контејнери представљају начин за олакшавање дистрибуције и поставке софтвера.
4. ***Теже праћење захтева који се простиру на више микросервиса*** – мерљивост (енг. *observability*) је способност система да пружи увид у своје унутрашње стање на основу његових спољних излаза. Записи, метрике и трагови познати су као три стуба мерљивости. Запис може бити било који забележен догађај неког сервиса. Агрегација скупа записа може произвести метрике. На неки начин, метрике одражавају стање система. У погледу безбедности, просечан број неисправних захтева за приступ по сату је метрика, на пример. Висок број вероватно указује да је систем под нападом или да је први слој одбране слаб. Може се конфигурисати упозорење на основу метрика. Ако број неисправних покушаја приступа за одређени микросервис пређе претходно постављен праг, систем може послати поруку упозорења. Трагови су такође базирани на записима, али пружају увид у различиту перспективу система. Они омогућују праћење захтева од тачке уласка у систем до тачке изласка из система. За разлику од монолитних апликација, захтев може ући у систем преко једног микросервиса и

обухватити више микросервиса пре него што напусти систем. Повезивање захтева између микросервиса је изазовно па је из тог разлога препорука да се користе дистрибуирани системи за праћење.

5. ***Одржавање креденцијала сервиса и полиса контроле приступа*** – сервер који не мења своје стање након покретања назива се непроменљив (енг. *immutable*) сервер. Најпопуларнији образац поставке за микросервисе је заснован на контејнерима. Сваки микросервис ради у свом контејнеру где је најбоља пракса да контејнер буде непроменљив. Другим речима, након што се контејнер покрене, не би требало да мења датотеке у свом систему датотека (енг. *file system*) или да чува стање током извршавања у самом контејнеру. Разлог коришћења непроменљивог сервера је лакша поставка система. У било ком тренутку може се креирати нови контејнер са основном конфигурацијом. Ако се оптерећење на микросервису повећава, на пример, потребно је више инстанци сервиса за хоризонтално скалирање. Пошто ниједна од покренутих инстанци контејнера не чува стање током извршавања, може се једноставно покренути нови контејнер да би прерасподелили оптерећење.

   У безбедној микросервисној архитектури, сам микросервис постаје тачка за примењивање безбедности. Као резултат, потребно је одржавати списак дозвољених клијената (вероватно других микросервиса) који могу приступити датом микросервису, као и низ полиса контроле приступа. Ови спискови нису статички, дозвољени клијенти и полисе контроле приступа стално се ажурирају. Са непроменљивим сервером, ови подаци не могу да се чувају у систему датотека сервера. Потребно је смислити процес који ће да гарантује да ће сервис приликом покретања да добије ажурирана подешавања. Сваки микросервис такође мора одржавати своје сопствене креденцијале, као што су сертификати. За бољу безбедност, ови креденцијали морају бити периодично ротирани. Могу се чувати са самим микросервисом (у систему датотека контејнера), али мора постојати начин да се убаце у микросервис приликом покретања.

6. ***Дељење корисничког контекста*** – у монолитним апликацијама, све интерне компоненте деле исту сесију, и све информације везане за корисника се добијају из те сесије. У микросервисној архитектури, ништа се не дели између микросервиса тако да кориснички контекст мора бити експлицитно прослеђен од једног микросервиса до другог. Изазов је изградити поверење између два микросервиса тако да примајући микросервис прихвати кориснички контекст прослеђен из позивајућег микросервиса. Потребан је и начин провере да кориснички контекст прослеђен између микросервиса није намерно измењен. Коришћење токена је један од популарних начина за дељење корисничког контекста између микросервиса. JWT се може посматрати као JSON порука којом се низ корисничких атрибута преноси од једног микросервиса до другог на криптографски безбедан начин.

7. ***Полиглотска архитектура захтева више експертизе из области безбедности у сваком тиму за развој*** – у микросервисној архитектури, сервиси комуницирају међусобно преко мреже. Они се не ослањају на имплементацију, већ на интерфејс сервиса. Ова ситуација омогућава сваком микросервису да изабере свој сопствени програмски језик и технолошки стек за имплементацију. У окружењу са више тимова, где сваки тим развија свој скуп микросервиса, сваки тим има флексибилност да изабере оптимални технолошки стек за своје потребе. Ова архитектура је позната као полиглотска архитектура. Полиготска архитектура чини безбедност изазовном. Из разлога што различити тимови користе различите технолошке стекове за развој, сваки

тим мора имати експерте из безбедности. Експерти треба да преузму одговорност за дефинисање најбољих безбедносних пракси, да истраже безбедносне алате за статичку анализу кода и динамичко тестирање, и да интегришу те алате у процес билдовања. Одговорности централизованог безбедносног тима који важи за целу организацију сада су расподељене међу различитим тимовима. У већини случајева, организације користе хибридни приступ, са централизованим безбедносним тимом и инжењерима у сваком тиму који се фокусирају на безбедност, а који развијају микросервисе.

ДОДАТАК Ц – ПРИНЦИП И АРХИТЕКТУРА НУЛТОГ ПОВЕРЕЊА

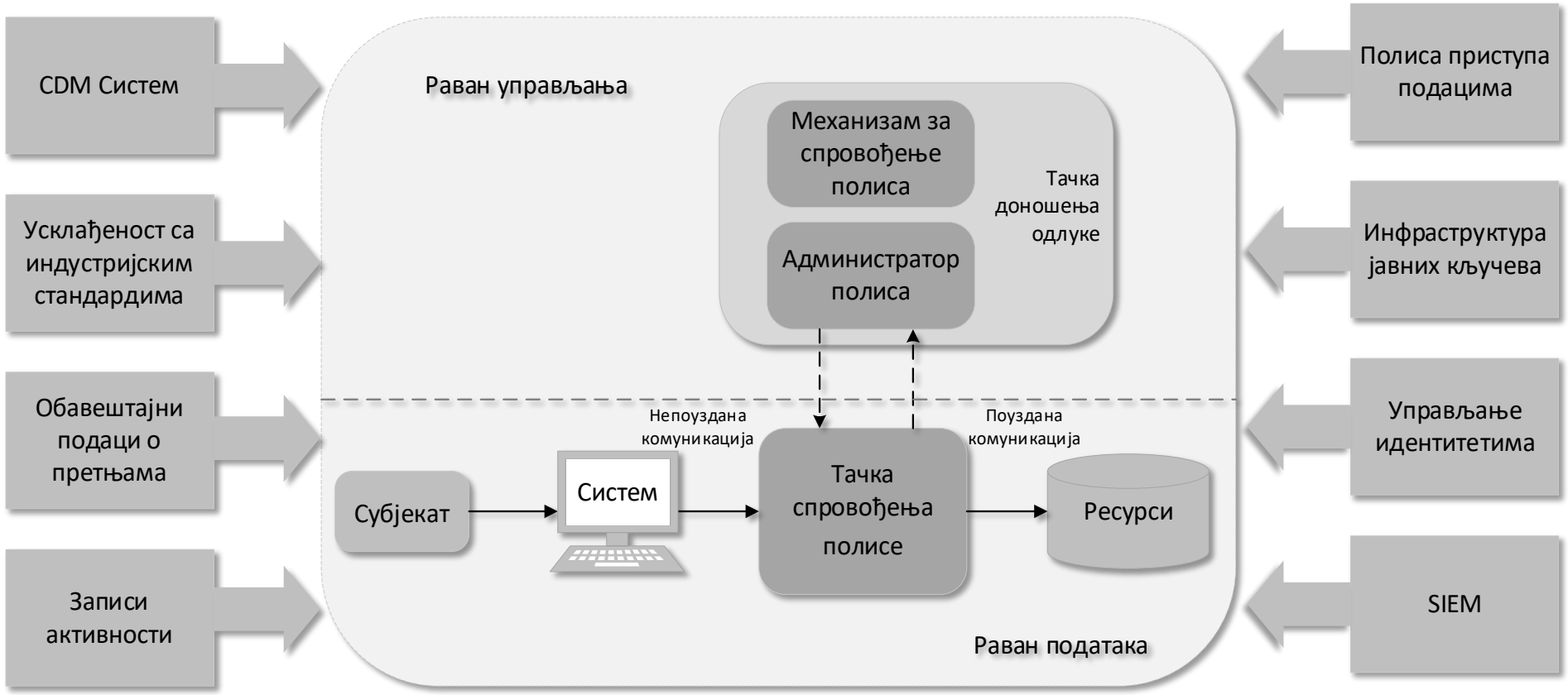
NIST је објавио документа који описују концепте принципа нултог поверења [83]. По њиховој дефиницији, у документу NIST SP 800-207, овај принцип представља „колекцију концепата и идеја дизајнираних да смање неизвесност у примени прецизних одлука о приступу са најмање привилегија по захтеву у информационим системима и услугама у мрежи која се сматра компромитованом". Поред тога, архитектура нултог поверења је "план сајбер безбедности предузећа које користи концепте нултог поверења и обухвата односе компоненти, планирање радних токова и политике приступа. Стога, предузеће са нултим поверењем је мрежна инфраструктура (физичка и виртуелна) и оперативне политике које су на снази у предузећу као производ плана архитектуре нултог поверења". Ова дефиниција се фокусира на суштину проблема, а то је циљ да се спречи неовлашћени приступ подацима и сервисима спровођењем контроле приступа која треба да буде што грануларнија. Односно, овлашћени и одобрени субјекти (корисник, апликација, сервис и уређај) могу приступити подацима искључујући све друге субјекте (тј. нападаче). Оно што је битно нагласити је да се принцип нултог поверења односи на приступ ресурсима (нпр. штампачима, рачунарским ресурсима, актуаторима, IoT), а не само на приступ подацима. Фокус је на аутентификацији, ауторизацији и смањењу зона имплицитног поверења, уз одржавање доступности и минимизирање временских кашњења у механизмима аутентификације. Правила приступа се чине што грануларнијим како би се спровеле најмање потребне привилегије за извршење радње у захтеву. Још једна кључна претпоставка принципа нултог поверења је да се поверење никада не даје имплицитно већ се мора континуирано евалуирати. Традиционално, сајбер безбедност је била фокусирана на одбрану периметра и аутентификовани субјекти су имали овлашћени приступ широком спектру ресурса једном када су доспели у унутрашњост мреже. Као резултат, неовлашћено латерално кретање у оквиру окружења је био један од највећих изазова.

У апстрактном моделу приступа, субјекту је потребан приступ ресурсима система. Приступ се одобрава преко тачке доношења одлука за полисе (*Policy Decision Point* – PDP) и одговарајуће тачке спровођења полисе (*Policy Enforcement Point* – PEP). Систем мора проверити да ли је субјект аутентичан и да је захтев валидан. PDP/PEP доноси одлуку да ли је субјекту дозвољен приступ ресурсу. Ово имплицира да се принцип нултог поверења примењује на две основне области: аутентификацију и ауторизацију. Предузећа треба да развију и одржавају динамичке полисе засноване на ризику за приступ ресурсима и да успоставе систем који ће осигурати да се те полисе правилно и доследно спроводе за појединачне захтеве за приступ ресурсима. Ово значи да предузеће не би требало да се ослања на подразумевану поузданост где, ако је субјект испунио основни ниво аутентификације (нпр. пријављивање на систем), сви наредни захтеви за ресурсима се

сматрају подједнако валидним. „Зона имплицитног поверења“ представља област у којој су сви ентитети поуздани бар на нивоу последње PDP/PEP капије. Са друге стране, PDP/PEP примењује скуп контрола тако да сав саобраћај иза има заједнички ниво поверења. PDP/PEP не може применити додатне политике изван своје локације у току саобраћаја. Да би PDP/PEP био што конкретнији, зона имплицитног поверења мора бити што мања. Принцип нултог поверења пружа сет принципа и концепата који подразумевају приближавање PDP/PEP-ова ресурсу. Идеја је да се експлицитно аутентификују и ауторизују сви субјекти, средства и радни токови који чине предузеће.

Логичке компоненте архитектуре нултог поверења

Постоји велики број логичких компоненти које чине архитектуру нултог поверења. Ове компоненте могу бити сервиси у локалном окружењу или сервиси у рачунарском облаку. Модел приказан на слици 15 приказује односе и интеракцију између компоненти.



Слика 15 – Основне компоненте архитектуре нултог поверења [83]

Опис компоненти:

- ***Механизам за спровођење полиса*** (енг. *Policy engine* – PE): Ова компонента је одговорна за доношење коначне одлуке о одобравању приступа ресурсу за одређени субјект. PE користи полису предузећа, као и улазне податке из спољних извора (нпр. CDM системи, службе за обавештавање о претњама описане испод) као улаз у алгоритам поверења да би одобрио, одбио или опозвао приступ ресурсу. Сервис полисе је упарен са компонентом администратора полисе. Сервис полисе доноси и бележи одлуку (као одобрену или одбијену), а администратор полисе је спроводи.

- ***Администратор полиса*** (енг. *Policy administrator*, PA): Ова компонента је одговорна за успостављање и/или прекидање комуникационог пута између субјекта и ресурса (путем команди релевантним за PEP). Генерисала би сваки аутентификациони токен специфичан за сесију или креденцијале које клијент користи за приступ ресурсу предузећа. Тесно је повезана са PE и ослања се на његову одлуку да дозволи или одбије сесију. Ако је сесија ауторизована и захтев аутентификован, PA конфигурише PEP да дозволи почетак сесије. Ако је сесија одбијена (или је претходно одобрење опозвано), PA сигнализира PEP да прекине везу. Неке имплементације могу третирати PE и PA као једну услугу; овде су подељени на своје две логичке компоненте. PA комуницира са PEP приликом креирања комуникационог канала. Ова комуникација се обавља преко контролне равни (енг. *control plane*).

- ***Тачка спровођења полисе*** (енг. *Policy enforcement point*, PEP): Овај систем је одговоран за омогућавање, надгледање и на крају прекидање веза између субјекта и ресурса предузећа. PEP комуницира са PA ради прослеђивања захтева и/или примене ажурираних полиса од PA. Ово је једна логичка компонента у архитектури нултог поверења, али може бити подељена на две различите компоненте: клијентску страну (нпр. агент на лаптопу) и страну ресурса (нпр. компонента улаза испред ресурса која контролише приступ) или једну преносну компоненту која делује као чувар комуникационих путева. Изван PEP-а је зона поверења на којој је постављен ресурс предузећа.

Поред основних компоненти у предузећу које имплементира архитектуру нултог поверења, неколико извора података пружа улазне податке и правила полиса које сервис полиса користи приликом доношења одлука о приступу. Ови извори укључују локалне изворе података, као и спољне (тј. неконтролисане или некреиране од стране предузећа) изворе података. Ови извори могу укључивати:

- ***Систем за континуирану дијагностику и ублажавање*** (енг. *Continuous diagnostics and mitigation,* CDM): Овај систем прикупља информације о тренутном стању средстава предузећа и примењује ажурирања на конфигурационе и софтверске компоненте. CDM систем предузећа пружа сервису полисе информације о средству које је послало захтев за приступ, као што су да ли је коришћен одговарајући закрпљени ОС, интегритет софтверских компоненти одобрених од стране предузећа или присуство неодобрених компоненти и да ли средство има познате рањивости. CDM системи су такође одговорни за идентификацију и потенцијално спровођење подскупа полиса на уређајима који нису у власништву предузећа, а који су активни на инфраструктури предузећа.

- ***Систем усклађености са индустријским стандардима***: Овај систем осигурава да предузеће остане усклађено са било којим регулаторним режимом под који може пасти. Ово укључује сва правила полисе која предузеће развија како би осигурало усклађеност.

- ***Извори обавештајних података о претњама***: Ови извори пружају информације из унутрашњих или спољних извора који помажу сервису полисе у доношењу одлука о приступу. Ово могу бити вишеструке услуге које узимају податке из унутрашњих и/или вишеструких спољних извора и пружају информације о новооткривеним нападима или рањивостима. Ово такође укључује новооткривене недостатке у софтверу, новоидентификовани малвер и пријављене нападе на друга средства којима би сервис полисе требао да онемогући приступ.

- ***Дневници активности мреже и система***: Овај систем предузећа агрегира записе средстава, мрежни саобраћај, радње приступа ресурсима и друге догађаје који пружају повратне информације у реалном (или скоро реалном) времену о безбедносном статусу информационих система предузећа.

- ***Полисе приступа подацима***: Ово су атрибути, правила и полисе о приступу ресурсима предузећа. Овај скуп правила може бити кодиран у (путем интерфејса за управљање) или динамички генерисан од стране сервиса полиса. Ове полисе су полазна тачка за ауторизацију приступа ресурсу јер обезбеђују основне привилегије приступа за налоге и апликације/сервисе у предузећу. Ове полисе треба да буду засноване на дефинисаним улогама и потребама организације.

- ***Предузетничка инфраструктура јавног кључа*** (енг. *Public key infrastructure*, PKI): Овај систем је одговоран за генерисање и евидентирање сертификата које предузеће издаје ресурсима, субјектима, сервисима и апликацијама. Ово такође укључује глобални екосистем ауторитета сертификата и Федерални PKI, који могу али не морају бити интегрисани са предузетничким PKI. Ово такође може бити PKI који није заснован на X.509 сертификатима.

- ***Систем управљања идентификацијом***: Овај систем је одговоран за креирање, чување и управљање корисничким налозима и записима идентитета у предузећу. Овај систем садржи неопходне информације о субјекту (нпр. име, адреса електронске поште, сертификати) и друге карактеристике предузећа као што су улога, атрибути приступа и додељена средства. Овај систем често користи друге системе (као што је PKI) за артефакте повезане са корисничким налозима.

- ***Систем за управљање безбедносним информацијама и догађајима*** (SIEM): Овај систем прикупља информације усредсређене на безбедност за каснију анализу. Ови подаци се затим користе за усавршавање полиса и упозоравање на могуће нападе на средства предузећа.

Архитектура нултог поверења је дизајнирана и развијена са поштовањем следећих основних постулата принципа нултог поверења [83]:

1. Сви **извори података** и **рачунарске услуге** се сматрају ресурсима – Мрежа може бити састављена од више класа уређаја. Такође, предузеће може одлучити да

посматра уређаје у личном власништву као ресурсе ако они могу приступити ресурсима у власништву предузећа.

2. Сва **комуникација** је безбедна без обзира на мрежну локацију – Сама мрежна локација не подразумева поузданост. Захтеви за приступ из компоненти које се налазе у инфраструктури мреже у власништву предузећа морају испунити исте безбедносне захтеве као захтеви за приступ и комуникацију из било које друге мреже која није у власништву предузећа. Другим речима, поверење не би требало аутоматски да се додељује на основу тога да ли је уређај у мрежној инфраструктури предузећа. Сва комуникација треба да се обавља на најбезбеднији могући начин, да заштити поверљивост и интегритет, и да обезбеди аутентификацију извора.

3. **Приступ ресурсима** предузећа се додељује **на нивоу сесије** – Поверење се евалуира пре него што се приступ одобри. Такође, приступ би требало да се одобри са најмањим привилегијама потребним да се задатак изврши. Аутентификација и ауторизација за један ресурс неће аутоматски дати приступ различитом ресурсу.

4. **Приступ ресурсима** одређује се **динамичком полисом** – укључујући видљиво стање идентитета клијента, апликације/сервиса и субјекта који захтева приступ – може укључивати и друге атрибуте понашања и околине. Организација да би заштитила ресурсе треба прво да их дефинише, да наведе ко су њени чланови и који ниво приступа ресурсима ти чланови имају. За принцип нултог поверења, идентитет клијента може представљати кориснички налог (или идентитет сервиса) и све повезане атрибуте које је предузеће додељивало том налогу за аутентификацију. Полиса је скуп правила приступа на основу атрибута које организација додељује субјекту, податку или апликацији. Атрибути могу укључивати факторе као што су локација мреже из које је захтев послат, време, пријављени активни напади итд. Ова правила и атрибути засновани су на потребама пословног процеса и прихватљивом нивоу ризика. Полисе приступа ресурсима и дозволе за акције могу варирати у зависности од осетљивости ресурса/података. Принципи најмање привилегије се примењују како би се ограничила и видљивост и доступност.

5. **Предузеће надгледа и мери интегритет и безбедносни статус** свих сопствених и повезаних уређаја – Ниједан уређај се по природи не сматра поузданим. Предузеће оцењује безбедносни статус уређаја приликом евалуације захтева за приступ ресурсима. Предузеће које имплементира архитектуру нултог поверења треба да успостави CDM или сличан систем за надгледање стања уређаја и апликација, и треба да примењује закрпе/исправке по потреби. Средства за која се утврди да су компромитована, да имају познате рањивости и/или да нису управљана од стране предузећа могу бити третирана другачије (укључујући ускраћивање свих веза ка ресурсима предузећа) у односу на уређаје у власништву или повезане са предузећем, а који се сматрају да су у најбезбеднијем стању. Ово може такође важити за повезане уређаје (нпр. уређаје у личном власништву) којима може бити дозвољен приступ неким ресурсима, али не и другима. Ово захтева постојање робусног система надгледања и извештавања који обезбеђује податке о тренутном стању ресурса предузећа.

6. Сва **аутентификација** и **ауторизација** ресурса је динамичка и строго спровођена пре него што је дозвољен приступ – Ово је стални циклус добијања приступа,

скенирања и процене рањивости, прилагођавања и континуираног процењивања поверења у текућој комуникацији. Предузеће које имплементира архитектуру нултог поверења треба да има системе за управљање идентитетом, креденцијалима и приступом (енг. *Identity, Credential, and Access Management,* ICAM), као и системе за управљање средствима. Ово укључује вишефакторску аутентификацију за приступ неким или свим ресурсима предузећа. Континуирано надгледање са могућом поновном аутентификацијом и поновном ауторизацијом се одвија током корисничких трансакција, као што је дефинисано и спроведено у полиси (нпр. на основу времена, нови захтев за ресурсом, модификација ресурса, откривена аномалија у активности субјекта) која настоји да постигне равнотежу између безбедности, доступности, употребљивости и економичности.

7. **Предузеће прикупља што више информација о тренутном стању средстава, мрежне инфраструктуре и комуникација** и користи их за побољшање свог безбедносног стања – Предузеће треба да прикупља податке о безбедносном стању средстава, мрежном саобраћају и захтевима за приступ, да обрађује те податке и користи увиде добијене из њих за побољшање креирања и спровођења полиса. Ови подаци се такође могу користити за давање контекста захтевима за приступ од стране субјеката.

Постоје неке основне претпоставке за мрежну конективност за сваку организацију која користи архитектуру нултог поверења у планирању и поставци мреже. Неке од ових претпоставки се односе на мрежну инфраструктуру у власништву предузећа, а неке се односе на ресурсе у власништву предузећа који раде на мрежној инфраструктури која није у власништву предузећа (нпр. јавни Wi-Fi или јавни пружаоци услуга у рачунарском облаку). **Мрежа у предузећу које имплементира архитектуру нултог поверења** треба да буде развијена са следећим претпоставкама.

1. Цела приватна мрежа предузећа се не сматра зоном имплицитног поверења – Средства увек треба да се понашају као да је нападач присутан на мрежи предузећа, а комуникација треба да се обавља на најсигурнији могући начин. Ово подразумева акције као што су аутентификација свих веза и енкриптовање целог саобраћаја.
2. Уређаји на мрежи можда нису у власништву предузећа нити их је могуће конфигурисати од стране предузећа – Посетиоци и/или уговорени сервиси могу укључивати средства која нису у власништву предузећа, а која требају приступ мрежи ради обављања својих улога. Ово укључује полисе коришћења сопствених уређаја (енг. *bring-your-own-device, BYOD*) које омогућавају субјектима предузећа да користе уређаје који нису у власништву предузећа за приступ ресурсима предузећа.
3. Ниједан ресурс није по природи поуздан – Сваки ресурс мора имати евалуирану безбедносну оцену преко PEP пре него што се одобри захтев за ресурсом у власништву предузећа. Ова оцена треба да буде важећа током трајања сесије. Уређаји у власништву предузећа могу имати артефакте који омогућавају аутентификацију и пружају ниво поверења већи него исти захтев који долази са уређаја који нису у власништву предузећа. Креденцијали субјекта сами по себи нису довољни за аутентификацију уређаја на ресурс предузећа.
4. Нису сви ресурси предузећа у инфраструктури која је у власништву предузећа – Ресурси укључују удаљене субјекте предузећа као и сервисе у рачунарском облаку. Средства у власништву или под управом предузећа можда ће морати да користе

локалну (енг. *nonenterprise*) мрежу за основну повезаност и мрежне услуге (нпр. DNS резолуцију).

5. Удаљени субјекти и средства предузећа не могу потпуно веровати својој локалној мрежи – Удаљени субјекти треба да претпоставе да је локална мрежа (која није у власништву предузећа) нападачка. Средства треба да претпоставе да се сви саобраћаји надгледају и потенцијално мењају. Сви захтеви за повезивање треба да буду аутентификовани и ауторизовани, а сва комуникација треба да се обавља на најсигурнији могући начин (тј. обезбедити поверљивост, заштиту интегритета и аутентификацију извора).
6. Средства и радни токови који се крећу између инфраструктуре у власништву предузећа и оне које нису у власништву предузећа треба да имају конзистентну безбедносну полису и позицију – Средства и радни токови треба да задрже своју безбедносну позицију када се премештају са или у инфраструктуру у власништву предузећа. Ово укључује уређаје који прелазе са мрежа предузећа на мреже које нису у његовом власништву (тј. удаљени корисници). Такође, укључује радне токове који мигрирају из локалних дата центара на инстанце рачунарског облака које нису у власништву предузећа.

ДОДАТАК Д – БЕЗБЕДНОСНИ ЗАХТЕВИ ЗА ИКС

Критичне инфраструктурне морају да задовоље скуп функционалних услуга и захтева како би се обезбедиле добре перформансе и поузданост [100]. Ови захтеви укључују перформантност, интероперабилност, скалабилност, проширивост, доступност, поузданост, отпорност, сигурност, аутономију и самоопоравак, употребљивост, поверење и сарадњу између хетерогених објеката како би се решавале ненормалне и претеће ситуације уз одржавање толеранције на грешке и безбедност.

- ***Интероперабилност*** се односи на способност различитих система и уређаја да међусобно сарађују како би постигли заједнички циљ. Овим се постиже већа флексибилност у избору опреме, лакша интеграција нових технологија, смањење трошкова и повећање оперативне ефикасности. Интероперабилност се постиже имплементацијом система у складу са прихваћеним индустријским стандардом, коришћењем заједничких комуникационих протокола, употреба мидлверских решења која служе као интерфејси између различитих система и коришћењем апликационих програмских интерфејса који омогућавају апликацијама да комуницирају и деле податке на стандардни начин.
- Корисно је ако је одређени део ИКС одговоран за дефинисање и одржавање ***перформантности*** целокупног система. Управљање се фокусира на развој, имплементацију и придржавање безбедносних политика и техничких спецификација, као и приступ и доступност техничких и правних докумената.
- ***Скалабилност*** се односи на способност додавања или уклањања хардверских ресурса при повећаним оптерећењем. Постоје две врсте скалабилности, хоризонтална која подразумева додавање више јединица или чворова (сервера) у систем и вертикална где се постојећој јединици система додаје више ресурса (повећање меморије, процесорске снаге и слично). Додавање нових ресурса не би требало да доведе до промене у услугама које пружа критични систем.
- ***Екстензибилност*** је повезана са способношћу проширивања или измене софтверског система без потребе за великим променама у постојећој архитектури. Омогућава лако проширење система новим функционалностима, компонентама или модулима. Ово је важно за одрживост и дугорочну употребу система, јер омогућава његов развој и прилагођавање новим захтевима и технологијама.
- ***Доступност и поузданост*** су два уско везана концепта. Доступност одговара вероватноћи да систем испоручи услуге када су затражене. Обично се изражава као проценат времена у ком је систем функционалан током одређеног периода. Док поузданост представља вероватноћу да систем доследно извршава своје функције без грешака и да његова доступност не опадне током временског периода. Другим речима,

поузданост представља метрику колико је систем стабилан и колико често долази до кварова или грешака.

- ***Квалитет услуге*** је такође важно својство јер би прекид или измена система услед кварова, инцидената, грешака или рањивости могли угрозити рад целе инфраструктуре. За развој одговарајуће стратегије квалитета услуге за ИКС, препоручљиво је разматрати додатне параметре као што су ниво хетерогености система, променљива природа и интерактивност окружења, топологија мреже, слабости повезане са објектима, као и међусобне зависности између чворова и система. Ово би омогућило прилагођавање суштинских параметара и дизајнирање робусних инфраструктура са способношћу да контролишу грешке и инциденте.
- ***Отпорност и робусност*** су својства која помажу у суочавању са штетним или претећим ситуацијама. Уопштено, систем под претњом треба да гарантује своју функционалност у сваком тренутку, чак и када су одређени делови система озбиљно компромитовани. Квар може покренути каскадни ефекат због интерних зависности које постоје између ресурса и елемената система.
- ***Сигурносно-критични аспекти*** морају бити разматрани како би се контролисали каскадни ефекти. Да би се спречило појављивање таквих ситуација, контролне мреже треба да укључе аутономне, динамичне и интелигентне приступе и да обезбеде превенцију и одговор на ефикасан и правовремени начин.
- Још једно важно својство је ***употребљивост***. Сваки корисник мора бити у могућности да интерагује са системом путем интуитивног интерфејса. Ово значи да би кориснички интерфејси требало да буду дизајнирани тако да информације (као што су аларми и сензорска очитавања) буду лаке за разумевање и да омогуће опције за брже извршавање критичних операција. Поред тога, хетерогеност окружења, присуство различитих мрежа, топологија и уређаја, као и поставка разноврсних услуга и апликација не би требало да утичу на континуитет пословања и оперативне активности.
- ***Сарадња између објеката*** је од кључног значаја у хетерогеним окружењима. На пример, сваки активни објекат у систему мора знати како да сарађује са другим објектима на безбедан и транспарентан начин, и како да извршава своје задатке. Поред тога, сви објекти треба да буду поуздани и да верују у размену информација како би се обезбедили брзи одговори у неповољним сценаријима. Поверење може бити проширено и на контексте апликација где нове технологије и инфраструктуре играју суштинску улогу. Ако се, на пример, резервне инстанце система налазе у инфраструктури рачунарског облака, критичне инфраструктуре морају имати поверење у инфраструктуру рачунарског облака и њене елементе како би се изводиле операције управљања.
- ***Толеранција на грешке*** је захтев који треба разматрати у сваком критичном окружењу како би се осигурао континуитет пословања у случају грешака у хардверу и софтверу. Један начин за контролу грешака је преко строгих безбедносних политика, одрживости и тестирања заснованих на процесима валидације и верификације, заједно са редунданцијом и динамичким приступима за откривање грешака, враћање у стање пре грешке и уклањање грешака. Ова решења имају више смисла у окружењима која укључују различите типове мрежа и многобројне интерактивне објекте. На крају, безбедносне аспекте треба решавати у целокупној SCADA архитектури како би се осигурала доступност, интегритет и поверљивост информација и ресурса.

ДОДАТАК Е – ПРОТОКОЛИ OAUTH2.0 И OIDC

OAuth 2.0 је протокол за ауторизацију који је дефинисан у RFC 6749 [100]. Његов основни фокус је омогућавање приступа ресурсима у име корисника, без потребе да апликација директно прикупља или чува корисничке креденцијале, као што су корисничко име и лозинка. Овај приступ значајно повећава сигурност и приватност корисника, јер омогућава да треће стране добију ограничен приступ само специфичним ресурсима на одређено време. OAuth 2.0 подржава неколико различитих токова ауторизације, од којих су следећа два од интереса за ову докторску дисертацију:

- **Authorization Code Flow with Proof Key for Code Exchange (PKCE)** – дефинисан је у RFC 7636 [101]. Омогућава безбедно добијање приступног токена (енг. *access token*) преко посредног механизма, коришћењем ауторизационог кода. PKCE гарантује спречавање злоупотребе ауторизационог кода ако га неко пресретне током процеса ауторизације. Кораци за добављање приступног токена:

  1) **Креирање потврђивача кода** (енг. *Code Verifier*) **–** апликација прво креира криптографски насумични стринг од најмање 43 карактера до највише 128 карактера који садржи комбинацију великих и малих слова, цифара и знакова као што су "-", ".", "_", "~". Овај стринг мора бити довољно насумичан да би спречио погађање од стране нападача.

  2) **Креирање изазова кода** (енг. *Code Challenge*) **–** апликација затим ради хеширање потвђивача кода користећи SHA-256 алгоритам, након чега се хеш резултат кодира у base64 формат.

  3) Апликација шаље изазов кода заједно са **захтевом за ауторизацију** и својим идентификатором на ауторизациони сервер преко HTTPS протокола.

  4) Након што се корисник аутентификује на серверу, ауторизациони сервер обрађује захтев и **шаље ауторизациони код** назад клијенту, при чему бележи изазов кода и метод трансформације (у овом случају SHA-256).

  5) Након добијања ауторизационог кода, апликација треба да **размени добијени код за приступни токен**. Шаље захтев на ауторизациони сервер где поред кода шаље и потврђивач кода.

  6) Ауторизациони сервер трансформише примљени потврђивач кода истом методом која је коришћена за добијање изазова кода и пореди резултат са претходно сачуваним изазовом кода. Ако су вредности једнаке, сервер издаје приступни токен. Ако нису, захтев се одбија.

- **Client Credentials Flow** – дефинисан у RFC 6749 [100], користи се када апликација треба да приступи ресурсима у своје име, а не у име корисника. Овај ток је најчешће примењен у случајевима када сервери међусобно комуницирају. За аутентификацију према серверу могу се користити сертификати који су везани за приступни токен. RFC 8705 [102] детаљно описује механизам аутентификације клијената, токене за приступ и освежавање, користећи узајамну аутентификацију преко TLS уз X.509 сертификате. OAuth клијентима је омогућен механизам за аутентификацију на серверу за ауторизацију користећи узајамни TLS, који се може заснивати на самопотписаним сертификатима или PKI. OAuth серверима за ауторизацију је такође омогућен начин за везивање приступних токена за TLS сертификат клијента. Ово омогућава заштићеним ресурсима у оквиру OAuth система да провером потврде осигурају да је приступни токен који им је послат издала овлашћена страна која га представља.

OpenID Connect (OIDC) проширује могућности OAuth 2.0 додавањем механизма за аутентификацију, чиме омогућава апликацијама да потврде идентитет корисника, поред тога што добијају приступ ресурсима. То се постиже путем ID токена, који садржи структуриране податке о кориснику, као што су јединствени идентификатор, име, адреса е-поште и друге релевантне информације. За разлику од само ауторизације у OAuth 2.0, OIDC осигурава да апликација може поуздано идентификовати ко је корисник који приступа ресурсима. Ово је посебно корисно у контексту пријављивања корисника на различите сервисе (енг. *Single Sign-On,* SSO).

План третмана података

Назив пројекта/истраживања
Развој безбедне микросервисне архитектуре у критичним инфраструктурним системима
Назив институције/институција у оквиру којих се спроводи истраживање
а) **Универзитет у Новом Саду, Факултет Техничких Наука** б) в)
Назив програма у оквиру ког се реализује истраживање
Истраживање се реализује у оквиру израде докторске дисертације на студијском програму Енергетика, електроника и телекомуникације.
1. Опис података

1.1 Врста студије

Укратко описати тип студије у оквиру које се подаци прикупљају

Докторска дисертација

_____

_____

_____

1.2 Врсте података

а) квантитативни

б) **квалитативни**

1.3. Начин прикупљања података

а) анкете, упитници, тестови

б) клиничке процене, медицински записи, електронски здравствени записи

в) генотипови: навести врсту _____

г) административни подаци: навести врсту _____

д) узорци ткива: навести врсту_____

ђ) снимци, фотографије: навести врсту_____

е) текст, навести врсту _**литература у области истраживања**_____

ж) мапа, навести врсту _____

з) остало: описати _**рачунарски експерименти**_____

1.3 Формат података, употребљене скале, количина података

1.3.1 Употребљени софтвер и формат датотеке:

а) Excel фајл, датотека _____

b) SPSS фајл, датотека _____

c) **PDF фајл, датотека _.pdf**_____

d) **Текст фајл, датотека _.docx**_____

e) **JPG фајл, датотека _.jbg**_____

f) **Остало, датотека _.xml, .html**_____

1.3.2. Број записа (код квантитативних података)

а) број варијабли _____

б) број мерења (испитаника, процена, снимака и сл.) _____

1.3.3. Поновљена мерења

а) да

б) **не**

Уколико је одговор да, одговорити на следећа питања:

а) временски размак између поновљених мера је _____

б) варијабле које се више пута мере односе се на _____

в) нове верзије фајлова који садрже поновљена мерења су именоване као _____

Напомене: _____

Да ли формати и софтвер омогућавају дељење и дугорочну валидност података?

а) ***Да***

б) Не

Ако је одговор не, образложити _____

_____

2. Прикупљање података

2.1 Методологија за прикупљање/генерисање података

2.1.1. У оквиру ког истраживачког нацрта су подаци прикупљени?

а) експеримент, навести тип _**рачунарски експеримент**_____

б) корелационо истраживање, навести тип _____

ц) анализа текста, навести тип _**анализа доступне литературе**_____

д) остало, навести шта _____

2.1.2 Навести врсте мерних инструмената или стандарде података специфичних за одређену научну дисциплину (ако постоје).

_____

_____

2.2 Квалитет података и стандарди

2.2.1. Третман недостајућих података

а) Да ли матрица садржи недостајуће податке? Да **Не**

Ако је одговор да, одговорити на следећа питања:

а) Колики је број недостајућих података? _____

б) Да ли се кориснику матрице препоручује замена недостајућих података? Да Не

в) Ако је одговор да, навести сугестије за третман замене недостајућих података

_____

2.2.2. На који начин је контролисан квалитет података? Описати

_____

**Квалитет података је контролисан поређењем експерименталних и теоријских података**

2.2.3. На који начин је извршена контрола уноса података у матрицу?

_____

_____

3. Третман података и пратећа документација

3.1. Третман и чување података

3.1.1. Подаци ће бити депоновани у _***Универзитет у Новом Саду***_ *репозиторијум.*

3.1.2. URL адреса *https://www.cris.uns.ac.rs/searchDissertations.jsf*

3.1.3. DOI _____

3.1.4. Да ли ће подаци бити у отвореном приступу?

а) ***Да***

б) *Да, али после ембарга који ће трајати до* _____

в) *Не*

Ако је одговор не, навести разлог _____

3.1.5. Подаци неће бити депоновани у репозиторијум, али ће бити чувани.

Образложење

_____

_____

3.2 Метаподаци и документација података

3.2.1. Који стандард за метаподатке ће бити примењен? **Стандард који примењује Репозиторијум докторских дисертација Универзитета у Новом Саду**

3.2.1. Навести метаподатке на основу којих су подаци депоновани у репозиторијум.

_____

_____

Ако је потребно, навести методе које се користе за преузимање података, аналитичке и процедуралне информације, њихово кодирање, детаљне описе варијабли, записа итд.

_____

_____

_____

_____

3.3 Стратегија и стандарди за чување података

3.3.1. До ког периода ће подаци бити чувани у репозиторијуму? _____

3.3.2. Да ли ће подаци бити депоновани под шифром? **Да** Не

3.3.3. Да ли ће шифра бити доступна одређеном кругу истраживача? **Да** Не

3.3.4. Да ли се подаци морају уклонити из отвореног приступа после извесног времена?

Да **Не**

Образложити

_____

_____

4. Безбедност података и заштита поверљивих информација

Овај одељак МОРА бити попуњен ако ваши подаци укључују личне податке који се односе на учеснике у истраживању. За друга истраживања треба такође размотрити заштиту и сигурност података.

4.1 Формални стандарди за сигурност информација/података

Истраживачи који спроводе испитивања с људима морају да се придржавају Закона о заштити података о личности *(https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html)* и одговарајућег институционалног кодекса о академском интегритету.

4.1.2. Да ли је истраживање одобрено од стране етичке комисије? Да **Не**

Ако је одговор Да, навести датум и назив етичке комисије која је одобрила истраживање

_____

4.1.2. Да ли подаци укључују личне податке учесника у истраживању? Да **Не**

Ако је одговор да, наведите на који начин сте осигурали поверљивост и сигурност информација везаних за испитанике:

а) Подаци нису у отвореном приступу

б) Подаци су анонимизирани

ц) Остало, навести шта

_____

_____

5. Доступност података

5.1. Подаци ће бити

а) ***јавно доступни***

б) доступни само уском кругу истраживача у одређеној научној области

ц) затворени

Ако су подаци доступни само уском кругу истраживача, навести под којим условима могу да их користе:

_____

_____

Ако су подаци доступни само уском кругу истраживача, навести на који начин могу приступити подацима:

_____

_____

5.4. Навести лиценцу под којом ће прикупљени подаци бити архивирани.

ауторство - некомерцијално_____

6. Улоге и одговорност

6.1. Навести име и презиме и мејл адресу власника (аутора) података

Марина Станојевић (marina.stanojevic@uns.ac.rs)_____

6.2. Навести име и презиме и мејл адресу особе која одржава матрицу с подацима

Марина Станојевић (marina.stanojevic@uns.ac.rs)_____

6.3. Навести име и презиме и мејл адресу особе која омогућује приступ подацима другим истраживачима

Марина Станојевић (marina.stanojevic@uns.ac.rs)_____