VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

IMPLEMENTACIJA MOBILE DEVICE MANAGEMENT SISTEMA V PODJETJU JÖBSTL

Kandidat: Marko Novak

Vrsta študija: študent izrednega študija

Študijski program: Računalništvo

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

Mentor v podjetju: Sergej Jamnikar, dipl. inž. rač. in inf.

Lektor: Jožica Vršič Novoselnik, prof. slov. in teol.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Marko Novak, sem avtor diplomskega dela z naslovom »Implementacija mobile device management sistema v podjetju Jöbstl«, ki sem ga napisal pod mentorstvom dr. Simona Žnidarja, univ.dipl.inž.el.

S svojim podpisom zagotavljam, da:

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

Maribor, avgust 2025 Podpis študenta:

ZAHVALA

Zahvaljujem se svojemu mentorju Sergeju Jamnikarju za strokovno usmerjanje, potrpežljivost in konstruktivne nasvete, ki so mi bili v veliko pomoč pri izdelavi diplomske naloge. Iskrena zahvala gre tudi moji ženi Doris in sinu Urhu – za njuno neomajno razumevanje, vzpodbujanje ter potrpežljivost v času študija in nastajanja naloge. Njuna podpora mi je pomenila veliko več, kot lahko izrazim z besedami.

POVZETEK

V zadnjih letih se je uporaba mobilnih naprav v podjetjih izrazito povečala, kar spodbuja potrebo po varnem in učinkovitem upravljanju teh naprav. Podjetje Jöbstl se pri digitalni transformaciji sooča z razdrobljenim nadzorom službenih in osebnih telefonov brez centralnih varnostnih politik. Takšne razmere povečujejo tveganje nepooblaščenega dostopa, izgube podatkov in zlorabe v primeru izgube ali kraje naprave. Implementacija sistema Mobile Device Management (MDM) je zato ključna za vzpostavitev centraliziranega nadzora, avtomatizirano nameščanje posodobitev ter oddaljeno upravljanje naprav.

Namen diplomske naloge je bil raziskati vpliv uvedbe MDM rešitve na varnost mobilnih naprav, operativno učinkovitost IT-infrastrukture in optimizacijo delovnih procesov v podjetju Jöbstl. Cilji so vključevali analizo obstoječega stanja v podjetju, izbor primerne rešitve, tehnično implementacijo, testiranje delovanja in pripravo strategij za odzivanje na morebitne incidente.

Raziskava je temeljila na analizi strokovne literature s področja MDM in kibernetske varnosti, študiji primera z analizo internih dokumentov ter opazovanjem delovnih procesov. Sledila je načrtovana implementacija izbrane rešitve in obsežno testiranje njenih funkcionalnosti ter varnostnih mehanizmov.

Glede na infrastrukturne in finančne omejitve podjetja je bila kot optimalna izbrana rešitev **ManageEngine Endpoint Central**. Platforma je bila lokalno nameščena na Windows Server 2022, integrirana z Active Directory in prilagojena tudi za uporabnike brez AD-računa. Konfigurirane so bile varnostne politike, kot so kompleksna gesla, šifriranje pomnilnika, omejitve za aplikacije in omrežje, vzpostavljena pa je bila tudi segmentacija omrežja in zaprto coniranje strežnika.

Rezultati so pokazali, da uvedba MDM sistema bistveno izboljša zaščito podatkov, poveča preglednost nad napravami ter zmanjša administrativno obremenitev IT-oddelka, kar predstavlja pomemben korak k večji digitalni varnosti in učinkovitosti podjetja.

Ključne besede: *Mobile Device Management, varnost mobilnih naprav, BYOD, Endpoint Central, kibernetska varnost*

ZUSAMMENFASSUNG

Implementierung eines Mobile-device-management-systems im unternehmen Jöbstl

In den letzten Jahren hat die Nutzung mobiler Geräte in Unternehmen deutlich zugenommen, was den Bedarf an einer sicheren und effizienten Verwaltung dieser Geräte verstärkt. Das Unternehmen Jöbstl steht im Rahmen seiner digitalen Transformation vor der Herausforderung einer fragmentierten Kontrolle über dienstliche und private Mobiltelefone ohne zentrale Sicherheitsrichtlinien. Solche Gegebenheiten erhöhen das Risiko eines unbefugten Zugriffs, von Datenverlusten sowie Missbrauch im Falle von Verlust oder Diebstahl eines Geräts. Die Implementierung eines Mobile-Device-Management-Systems (MDM) ist daher entscheidend, um eine zentralisierte Verwaltung, die automatisierte Installation von Updates sowie die Fernverwaltung der Geräte zu ermöglichen.

Ziel dieser Diplomarbeit war es, die Auswirkungen der Einführung einer MDM-Lösung auf die Sicherheit mobiler Geräte, die operative Effizienz der IT-Infrastruktur sowie die Optimierung von Arbeitsprozessen im Unternehmen Jöbstl zu untersuchen. Die Ziele umfassten die Analyse des bestehenden Zustands im Unternehmen, die Auswahl einer geeigneten Lösung, die technische Implementierung, die Funktionsprüfung sowie die Erstellung von Strategien zur Reaktion auf mögliche Sicherheitsvorfälle.

Die Untersuchung basierte auf einer Analyse der Fachliteratur im Bereich MDM und Cybersicherheit, einer Fallstudie mit Auswertung interner Dokumente sowie der Beobachtung von Arbeitsprozessen. Darauf folgten die geplante Implementierung der ausgewählten Lösung und umfangreiche Tests ihrer Funktionalitäten und Sicherheitsmechanismen.

Unter Berücksichtigung der infrastrukturellen und finanziellen Rahmenbedingungen des Unternehmens wurde ManageEngine Endpoint Central als optimale Lösung ausgewählt. Die Plattform wurde lokal auf einem Windows Server 2022 installiert, in Active Directory integriert und zusätzlich für Benutzer ohne AD-Konto angepasst. Es wurden Sicherheitsrichtlinien konfiguriert – darunter komplexe Passwörter, Speicherverschlüsselung, Einschränkungen für Anwendungen und Netzwerkzugriffe – sowie eine Netzwerksegmentierung und eine geschlossene Zonierung des Servers eingerichtet.

Die Ergebnisse zeigten, dass die Einführung des MDM-Systems den Datenschutz deutlich verbessert, die Transparenz über die Geräte erhöht und die administrative Belastung der IT-Abteilung reduziert. Dies stellt einen wichtigen Schritt zu mehr digitaler Sicherheit und Effizienz im Unternehmen dar.

Schlüsselwörter: *Mobile Device Management, Sicherheit mobiler Geräte, BYOD, Endpoint Central, Cybersicherheit*

KAZALO VSEBINE

KAZALO SLIK

KAZALO TABEL

SEZNAM KRATIC

MDM – Mobile Device Management

BYOD – Bring Your Own Device

CISO – Chief Information Security Officer

IT – Information Technology

DMZ – Demilitarized Zone

EPC – Endpoint Central

VPN – Virtual Private Network

TLS – Transport Layer Security

SSL – Secure Sockets Layer

HTTP – Hypertext Transfer Protocol

MITM – Man-in-the-Middle attack

Wi-Fi – Wireless Fidelity

MFA – Multi-Factor Authentication

SMS – Short Message Service

1 UVOD

V zadnjih letih se je uporaba mobilnih naprav v podjetjih močno povečala, kar kaže na naraščajočo potrebo po zagotavljanju varnega in učinkovitega upravljanja teh naprav. Mobilne naprave omogočajo zaposlenim večjo fleksibilnost in mobilnost pri delu, hkrati pa prinašajo izzive na področju varnosti in nadzora. Podjetje Jöbstl se pri svoji digitalni transformaciji sooča s kompleksnostjo upravljanja vedno večjega števila mobilnih naprav, ki se uporabljajo za dostop do internih sistemov in občutljivih podatkov. Neustrezno upravljanje teh naprav povečuje tveganje za nepooblaščen dostop, izgubo podatkov in druge kibernetske grožnje. Implementacija sistema Mobile Device Management (MDM) predstavlja ključno rešitev za obvladovanje teh izzivov, saj omogoča centraliziran nadzor, standardizirano konfiguracijo in celovito varnostno zaščito mobilnih naprav. S tem se zmanjšujejo varnostna tveganja, izboljšuje preglednost nad napravami in optimizira delo IT-oddelka. Poleg tega MDM omogoča hitrejše odzivanje na incidente, enostavnejše uvajanje posodobitev ter boljše upravljanje naprav v scenarijih, kjer se prepletata uporaba službenih in zasebnih telefonov. Ta diplomska naloga bo raziskala proces uvajanja MDM sistema v podjetju Jöbstl, vključno z analizo potreb in zahtev, pregledom varnostnih ukrepov ter oblikovanjem strategij za odzivanje na morebitne incidente. Rezultati bodo prispevali k oblikovanju celovite varnostne arhitekture podjetja ter krepitvi njegove odpornosti na sodobne kibernetske grožnje.

1.1 Opis področja in opredelitev problema

Namen diplomskega dela je raziskati vpliv implementacije MDM sistema v podjetju Jöbstl na varnost mobilnih naprav, operativno učinkovitost IT infrastrukture ter celostno optimizacijo delovnih procesov. Pri tem si želim pridobiti teoretična in praktična znanja o tem, kako lahko centralizirano upravljanje mobilnih naprav izboljša kibernetsko varnost in poslovno učinkovitost.

Glavni cilji naloge so:

- Analizirati trenutno stanje mobilnih naprav in njihove ranljivosti v podjetju Jöbstl.
- Izbrati in implementirati ustrezen MDM sistem, ki se bo vključil v obstoječo IT arhitekturo.
- Razviti celovit načrt za preverjanje in testiranje delovanja rešitve.
- Opredeliti varnostne ukrepe ter strategije odzivanja na morebitne incidente.

Osnovne trditve oziroma hipoteze, ki jih bo delo raziskovalo in katerih veljavnost bom potrdil ali ovrgel, so:

H1: Implementacija MDM sistema poveča varnost mobilnih naprav.

H2: Integracija MDM sistema v obstoječo IT arhitekturo izboljša operativno učinkovitost.

H3: Redno testiranje in spremljanje MDM sistema omogoča pravočasno odkrivanje varnostnih ranljivosti.

H4: Implementacija MDM sistema povečuje efektivnost dela zaposlenih in zmanjšuje stroške.

H5 – dodatna hipoteza (BTEC 2025 »Kibernetska varnost«): Implementacija večfaktorske avtentikacije izboljša varnost sistemov in zmanjša uspešnost social engineering napadov.

1.2 Namen, cilji in osnovne trditve

Namen diplomske naloge je bil poglobiti razumevanje sodobnih tehnologij ter pridobiti nova znanja s področja upravljanja mobilnih naprav. S tem pristopom sem si prizadeval razširiti svoje kompetence in ustvariti povezavo med teoretičnimi spoznanji ter praktičnimi izkušnjami na realnem primeru.

Cilj naloge je bil uspešno implementirati sistem MDM v podjetju Jöbstl, kar je omogočilo celovit nadzor nad mobilnimi napravami ter izboljšalo varnostno in operativno učinkovitost. S simulacijo različnih scenarijev delovanja sem preizkusil učinkovitost sistema ter identificiral morebitne priložnosti za optimizacijo.

Uvedba naprednega MDM sistema pozitivno vpliva na delovanje podjetja. Sistem okrepi varnost in administracijo mobilnih naprav, ter tudi povečuje zaupanje uporabnikov v tehnološke rešitve.

1.3 Predpostavke in omejitve

Vsi procesi implementacije sistema MDM v podjetju Jöbstl so potekali v skladu z načrtovanimi aktivnostmi in s podporo s strani organizacije.

Omejitev naloge je dostopnost podatkov, saj so številne informacije, povezane z interno infrastrukturo podjetja, konfiguracijami in varnostnimi politikami, opredeljene kot poslovna skrivnost. Zaradi tega niso bile vse podrobnosti objavljene ali pa so bile predstavljene v

anonimni ali prirejeni obliki. Prav tako ni bilo mogoče vključiti občutljivih internih poročil ali sistemskih dnevnikov, ki bi sicer lahko dodatno osvetlili delovanje sistema.

Omejitev je predstavljala tudi časovna komponenta izvedbe, saj so bile določene faze testiranj in analiz možne le v omejenem časovnem oknu zaradi poslovne dinamike podjetja. Kljub temu pa predstavljeni rezultati ponujajo zanesljivo osnovo za oceno uspešnosti implementacije sistema MDM in morebitne nadaljnje izboljšave.

1.4 Uporabljene raziskovalne metode

Pri pripravi te diplomske naloge sem uporabil naslednje raziskovalne metode:

- Analiza literature: prvi korak raziskave je temeljil na obsežni analizi strokovne literature. Pregledal sem akademske članke, uradne smernice in tehnične dokumente, ki obravnavajo področje MDM sistemov in kibernetske varnosti.
- Študija primera: delo vključuje podrobno analizo primera podjetja Jöbstl, kjer sem ocenil trenutno stanje upravljanja mobilnih naprav, njihove ranljivosti ter pridobil podatke o potrebah in pričakovanjih v zvezi z implementacijo MDM sistema.
- Načrtovanje in implementacija: naslednji del raziskave se je osredotočil na pripravo celovitega načrta za uvedbo izbranega MDM sistema. Vključeni so postopki izbire, konfiguracije in integracije rešitve v obstoječo IT infrastrukturo podjetja.
- Preverjanje in testiranje: zadnji del raziskave vključuje testiranje in preverjanje delovanja implementiranega sistema. Opredelil sem merljive kazalnike učinkovitosti, kot so odzivni čas na varnostne incidente, uspešnost nadzora mobilnih naprav in zmanjšanje tveganj. Ta faza omogoča analiziranje rezultatov ter primerjavo stanja pred in po uvedbi sistema.

2 CILJI RAZISKAVE

Glavni namen raziskave je analizirati, izbrati in implementirati ustrezno MDM rešitev, ki bo podjetju Jöbstl omogočila učinkovito upravljanje mobilnih naprav znotraj njihovega poslovnega okolja.

2.1 Pregled specifičnih ciljev raziskave

V okviru naloge sem zasledoval naslednje raziskovalne cilje:

- Analizirati obstoječe stanje upravljanja mobilnih naprav v podjetju, pri čemer je poudarek na ugotavljanju varnostnih ranljivosti, neučinkovitih postopkov ter tveganj, povezanih z uporabo odklenjenih naprav in BYOD pristopa.
- Raziskati in primerjati razpoložljive MDM rešitve, pri čemer sem ocenjeval njihove funkcionalnosti, varnostne možnosti, združljivost z obstoječo IT infrastrukturo podjetja in pogoje za lokalno implementacijo.
- Izbrati najbolj primerno MDM rešitev glede na potrebe in omejitve podjetja, pri čemer sem dal prednost sistemu, ki ne zahteva uporabe oblačne infrastrukture, omogoča celovit nadzor nad napravami ter zagotavlja visoko raven varnosti.
- Načrtovati, tehnično implementirati in testirati izbrano MDM rešitev, z namenom preveriti skladnost z varnostnimi standardi in njeno učinkovitost v realnem okolju podjetja Jöbstl.
- Oceniti vpliv uvedene rešitve na varnost, preglednost in operativno učinkovitost podjetja, pri čemer sem želel ugotoviti, v kolikšni meri MDM sistem izboljša obvladovanje tveganj in upravljanje digitalnih sredstev.

2.2 Povezava raziskovalnih ciljev s potrebami podjetja Jöbstl

Izbor ciljev raziskave je neposredno izhajal iz specifičnih potreb podjetja Jöbstl, ki je že pred začetkom raziskave zaznavalo številne izzive na področju upravljanja mobilnih naprav. Zaradi razpršene rabe mobilnih naprav, pri čemer se uporabljajo tako službeni kot osebni telefoni, podjetje ni imelo ustreznega pregleda nad tem, kdo uporablja katero napravo, katere aplikacije so nameščene in kakšne varnostne nastavitve so v uporabi. Takšna nepreglednost je oteževala tako tehnično podporo kot tudi izvajanje varnostnih politik, saj IT-oddelek ni imel centraliziranih podatkov o stanju naprav in njihovih konfiguracijah.

Službene naprave so bile popolnoma odklenjene, brez standardizirane zaščite ali možnosti oddaljenega dostopa, kar je predstavljalo veliko varnostno tveganje, zlasti ob morebitni izgubi ali kraji naprav. V takšnih primerih podjetje ni imelo možnosti takojšnjega zaklepa ali brisanja podatkov na daljavo, kar bi lahko preprečilo nepooblaščen dostop do občutljivih informacij. Poleg tega so bile nameščene aplikacije pogosto izven nadzora podjetja, kar je povečevalo možnost vnosa zlonamerne programske opreme ali nepooblaščenega prenosa podatkov.

Prav tako v podjetju ni bilo centralnega sistema za nadzor in posodabljanje mobilnih naprav, kar je oteževalo skladnost z varnostnimi pravili in upočasnjevalo odzivanje na incidente. Posodobitve operacijskih sistemov in varnostnih popravkov so bile prepuščene posameznim uporabnikom, kar je povzročalo neenotno zaščito in povečano izpostavljenost kibernetskim grožnjam. Vse te okoliščine so jasno pokazale potrebo po uvedbi celovite rešitve, ki bi omogočila centralizirano upravljanje, standardizacijo nastavitev ter učinkovito izvajanje varnostnih ukrepov na vseh napravah, ne glede na to, ali so v lasti podjetja ali zaposlenih.

3 METODOLOGIJA

3.1 Analiza obstoječe literature in raziskav na področju MDM sistemov

Analiza literature je temeljila na sistematičnem pregledu strokovnih člankov in tehničnih poročil, pridobljenih prek univerzitetnih baz podatkov in korporativnih virov. Za iskanje relevantnih virov sem uporabil ključne izraze, kot so “Mobile Device Management”, “endpoint security” in “enterprise mobility”.

3.2 Študija primera: Podjetje Jöbstl

Študija primera je izvedena z analizo internih dokumentov in neposrednega opazovanja delovnih procesov. Izbrani so bili zaposleni iz IT oddelka, logistike in pisarniški delavcev, ki uporabljajo mobilne naprave v službene namene. To je zagotovilo raznolikost glede upravljanja mobilnih naprav. Analiza je razkrila ključne nepravilnosti, kot so odsotnost centraliziranega nadzora, nerazporejene varnostne politike in ročni postopki posodabljanja, na podlagi katerih so bile opredeljene specifične zahteve za nadaljnji razvoj rešitve.

3.3 Načrtovanje, implementacija in testiranje MDM sistema

V fazi načrtovanja sem začel z določitvijo funkcionalnih in nefunkcionalnih zahtev, ki sem jih prepoznal v obstoječi literaturi in preko analize primera podjetja Jöbstl. S pomočjo sodelavcev smo oblikovali arhitekturo sistema, pri čemer smo poudarek dali zaščitnim protokolom in nadzoru dostopa. Ta faza je bila pomembna za pripravo tehničnega okvira, na katerem temelji celotna implementacija.

V naslednjem koraku sem pristopil k konkretni implementaciji MDM sistema. Sistem sem konfiguriral tako, da je omogočal sledenje in nadzor nad napravami znotraj podjetja Jöbstl. Celoten postopek je bil izveden v skladu s predhodno zastavljenimi tehničnimi zahtevami in najboljšimi praksami, kar je pripomoglo k nemotenemu delovanju celotnega sistema.

Zaključna faza je bilo testiranje, ki sem ga izvedel tako na funkcionalni kot na varnostni ravni. Pri testiranju sem preveril učinkovitost implementiranih funkcionalnosti in ocenil zanesljivost varnostnih mehanizmov.

4 TEORETIČNI PREGLED MOBILE DEVICE MANAGEMENT (MDM) SISTEMOV

4.1 Definicija in razvoj mobilnih naprav ter njihova vloga v sodobnih podjetjih

V sodobnem poslovnem okolju mobilne naprave niso več zgolj orodja za komunikacijo, temveč so postale integralni del digitalne infrastrukture, ki omogočajo neprekinjen dostop do podatkov in storitev. Mohiuddin in Akbar (2023) poudarjata, da so mobilne naprave evolvirale v kompleksne informacijske sisteme, katerih uporaba je močno povezana z naraščajočim trendom politike »prinesi svojo napravo (BYOD)« in uvajanjem oblačnih rešitev. Ta proces digitalne transformacije, ki je hkrati spodbudil povečanje produktivnosti in fleksibilnosti zaposlenih, zahteva natančno usklajevanje med poslovnimi procesi in IT varnostjo. Barthwal (2016) v svoji raziskavi o uporabi MDM v organizacijah dodaja, da se rast prometa mobilnih naprav ne more razložiti zgolj s tehnološkim napredkom, ampak je tudi odziv na spremembe v delovnih praksah in pričakovanjih sodobnih zaposlenih.

Priročnik kibernetske varnosti (2020) mobilne naprave opredeljuje kot prenosne informacijske sisteme, ki shranjujejo in prenašajo občutljive poslovne podatke prek nezanesljivih brezžičnih omrežij. Avtorji opozarjajo, da je zaradi te mobilnosti obvezna implementacija dodatnih varnostnih ukrepov: redno posodabljanje operacijskih sistemov, šifriranje shranjenih podatkov in komunikacij, večstopenjska avtentikacija ter segmentacija omrežja z uporabo VPN povezav. Poleg tega se navaja, da so ključni elementi učinkovitega MDM sistema centralizirano upravljanje dostopa, avtomatizirano nameščanje varnostnih popravkov in zmogljivosti za oddaljeno zaklepanje ter brisanje naprave v primeru izgube ali kraje.

4.2 Pregled obstoječih rešitev in tehnologij MDM

Na trgu se danes pojavljajo različne rešitve, ki prinašajo celovite pristope k upravljanju mobilnih naprav, pri čemer se vsaka rešitev prilagaja specifičnim potrebam posamezne organizacije. ManageEngine Endpoint Central omogoča centralizirano upravljanje endpoint naprav s funkcionalnostmi, kot so oddaljeno zaklepanje, geolokacijsko sledenje, avtomatizirano posodabljanje in nadzor aplikacij. Poleg tega nudi podrobno poročanje o stanju naprav, integracijo s priljubljenimi ITSM orodji ter razširljiv API za po meri izdelane delovne tokove, kar znatno zmanjša operativna tveganja in zagotavlja skladnost z internimi varnostnimi

politikami; to je posebej pomembno v podjetjih, kjer se mobilnost uporablja tako pri službenih kot pri BYOD modelih. (ManageEngine, 2024)

Omnissa Workspace ONE UEM Unified endpoint management je celovita, oblačna platforma za upravljanje mobilnih naprav, ki združuje nadzor naprav, aplikacij in omrežnih nastavitev. Rešitev omogoča avtomatizirano vpisovanje naprav, oskrbo s certifikati, upravljanje življenjskega cikla naprav in segmentacijo prometa na ravni posameznih aplikacij prek varovanih VPN tunelov. Samopostrežni portal uporabnikom olajša namestitev odobrenih aplikacij, medtem ko IT-oddelku zagotavlja podrobne vpoglede v skladnost naprav in centralizirano upravljanje varnostnih politik. (Omnissa, 2025)

Ivanti Neurons for MDM, se osredotoča na rigorozni "zero trust" varnostni model. Po podatkih z uradne strani leži njegova moč v ločevanju poslovnih in osebnih vsebin znotraj varovanih kontejnerjev, obveznem preverjanju skladnosti naprav z internimi varnostnimi zahtevami ter integraciji z rešitvami za zaznavanje in odzivanje na varnostne incidente. Poleg tega Ivanti neovirano avtomatizira nameščanje popravkov, konfiguracij in varnostnih politik na vseh podprtih platformah, kar zagotavlja hitro spremljanje in odzivanje v realnem času. (Ivanti, 2025)

4.3 Pomen varnosti v okviru MDM sistemov in IT infrastrukture

Zaradi obdelave občutljivih informacij in kritičnih poslovnih podatkov je varnost mobilnih naprav ključnega pomena. Učinkovit MDM sistem mora zagotavljati šifriranje podatkov tako na napravi kot med prenosom, saj to prepreči nepooblaščen dostop, če naprava pride v napačne roke. Večstopenjska avtentikacija dodatno krepi zaščito, saj zahteva vsaj dva neodvisna načina preverjanja pristnosti pred dostopom do poslovnih virov, kar zmanjša tveganje zlorabe. Možnost oddaljenega zaklepanja in brisanja omogoča takojšen odziv v primeru izgube ali kraje naprave, s čimer se prepreči razkritje občutljivih podatkov. Prav tako je nujno avtomatizirano nameščanje varnostnih popravkov, saj več kot 60 % uspešnih kibernetskih napadov izkorišča ranljivosti nepravočasno posodobljenih naprav (Boštjančič Pulko, et al., 2025). Stalno spremljanje dnevniških zapisov in avtomatizirano poročanje sta ključna za hitro odkrivanje anomalij ter sprotno ukrepanje (National Cybersecurity Authority of Greece, 2021). Uvedba celovitega MDM sistema prinaša strateške koristi pri nadzoru in zaščiti informacij, saj sistematično upravljanje in poročanje o skladnosti zmanjšuje operativna tveganja ter krepi zaupanje v IT okolje. (Barthwal, 2016)

Poleg osnovnih varnostnih mehanizmov MDM rešitve omogočajo tudi integracijo z informacijskimi sistemi za upravljanje varnostnih dogodkov in orodji za zaznavanje ter odzivanje na grožnje, kar podjetjem omogoča proaktivno spremljanje varnostnih incidentov ter avtomatizirano sprožanje ukrepov, kot so blokada ali karantena kompromitirane naprave. Dinamične preglede skladnosti sistem izvaja stalno in avtomatizirano, pri čemer redno preverja posodobljenost operacijskega sistema, pravila gesel in uporabo varnih komunikacijskih protokolov. Takšen pristop bistveno skrajša čas med zaznavo in odpravo ranljivosti ter krepi odpornost celotne IT infrastrukture. (National Cybersecurity Authority of Greece, 2021)

5 IMPLEMENTACIJA MDM SISTEMA

5.1 Analiza obstoječega stanja mobilnih naprav v podjetju

V podjetju Jöbstl trenutno ni bilo vzpostavljenega sistema za centralizirano upravljanje mobilnih naprav. Analiza obstoječega stanja je pokazala, da so se mobilne naprave uporabljajo brez kakršnekoli formalne politike. Službeni telefoni so bili v celoti odklenjeni, kar pomeni, da so imeli zaposleni popoln dostop do namestitve različnih aplikacij, brskanja po spletu brez omejitev in neomejeno porabo mobilnih podatkov. Takšen način uporabe je omogočal, da si je vsak zaposleni lahko namestil katerokoli aplikacijo, kar je lahko vodilo v nepravilno uporabo, izgubo kontrole nad namestitvijo programske opreme ter nepooblaščen dostop do občutljivih informacij.

Poleg službenih naprav se je v podjetju lahko uporabljala politika BYOD, pri kateri so zaposleni uporabljali svoje osebne telefone za opravljanje službenih nalog. V tovrstnih primerih so poslovni podatki in dokumenti pogosto pomešani z osebnimi vsebinami, kar dodatno zaplete zaščito informacij in otežuje nadzor nad varnostnimi nastavitvami. V podjetju ni obstajal enoten kontrolni mehanizem, ki bi omogočal avtomatizirano posodabljanje, namestitev aplikacij ali enostavno blokado naprav v primeru izgube ali kraje.

Ta razdrobljenost vodi v večje varnostne grožnje, saj se zaradi pomanjkanja centraliziranega nadzora ne morejo učinkovito izvajati varnostni ukrepi. Vse to je predstavljal resen problem za podjetje Jöbstl, kjer naraščajoča uporaba mobilnih naprav in nezmožnost nadzora pripeljeta do povečanja tveganj, povezanih z uhajanjem podatkov in morebitnimi vdori.

5.2 Izbor ustreznega MDM sistema za podjetje Jöbstl

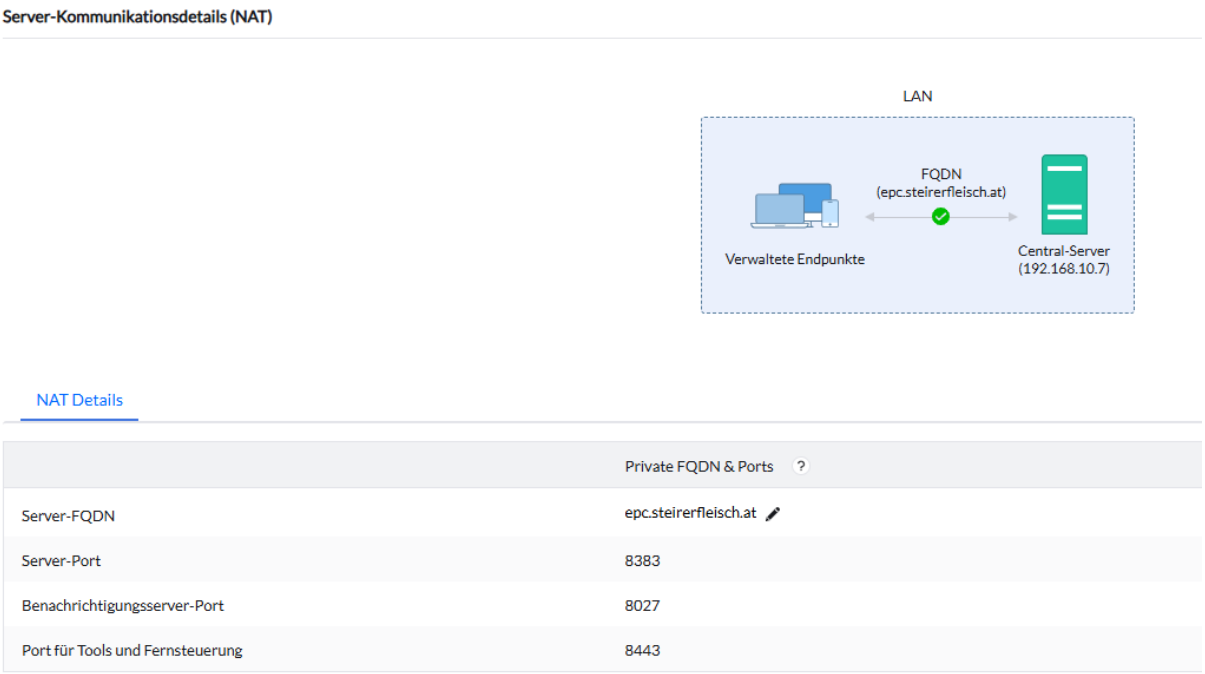
Podjetje Jöbstl je pri izbiri MDM rešitve izhajalo iz dveh ključnih zahtev: sistem mora delovati izključno na lastni infrastrukturi, saj vodstvo ne želi prehoda na oblačne storitve, hkrati pa so finančne omejitve pomemben dejavnik odločanja. Na eni strani se je izkazalo, da ponudniki, kot sta VMware Workspace ONE UEM in Ivanti Neurons for MDM, sicer ponujajo obsežne funkcionalnosti in visoko raven varnosti, vendar temeljita na modelu, ki predvideva drage vsakoletne licence in morebiti dodatne stroške za oblačno gostovanje in podpore. Podjetje Jöbstl potrebuje rešitve, kjer lahko obstoječi strežniki prek upravljalske konzole namestijo in vzdržujejo sistem brez doplačil za gostovanje, zato so ponudniki, ki zahtevajo lasten oblak ali zaračunavajo stroške za SaaS, odpadli.

Med preučevanimi lokalnimi rešitvami je izstopal ManageEngine Endpoint Central. Ta platforma omogoča namestitev celotnega MDM sistema na interne strežnike, pri čemer so stroški licenc za lokalno gostovanje večkrat nižji od podobnih modelov pri večjih ponudnikih. Poleg tega ManageEngine nudi modularno licenciranje, kar pomeni, da lahko podjetje najprej pridobi osnovni paket za upravljanje naprav in ga po potrebi postopoma nadgrajuje, ne da bi se takoj zavezal k velikim začetnim investicijam. V predhodnih analizah so se izkazale kot pomembne tudi obsežne možnosti integracije z Active Directory (AD), kar znižuje stroške implementacije in upravljanja uporabniških računov, saj je sinhronizacija in dodeljevanje pravic že v pomoč pri avtomatizaciji delovnih tokov.

Končna odločitev za ManageEngine Endpoint Central tako temelji na razmerju med ceno in zmogljivostjo. Rešitev združuje vse ključne funkcionalnosti MDM – oddaljeno zaklepanje in brisanje, geolokacijsko sledenje, avtomatsko posodabljanje, centralno nadzorovanje aplikacij in granulirane varnostne politike – hkrati pa ohranja stroške vzdrževanja in lastniške licence na zmerni ravni. Lokalna namestitev na že obstoječo strežniško infrastrukturo podjetja Jöbstl znižuje kapitalske izdatke, medtem ko modularno licenciranje omogoča, da se investicija razdeli čez več zaporednih obdobij. Tako je bil ManageEngine Endpoint Central prepoznan kot optimalna rešitev, saj ustreza varnostnim zahtevam, infrastrukturnim omejitvam in finančnim prioritetam podjetja.

5.3 Integracija MDM sistema v celotno IT arhitekturo podjetja

Pri vzpostavitvi lokalno gostovanega ManageEngine MDM sistema je vse potrebno izvedel CISO podjetja Jöbstl, ki je strežnik integriral v obstoječo arhitekturo kot virtualni stroj Windows Server 2022 Datacenter. On je najprej poskrbel za varnostno utrditev strežnika v ločeni omrežni coni in namestitev vseh predpogojev. Na požarnem zidu je omogočil samo tiste vhodne porte, ki jih uporablja MDM konzola in agenti na napravah – port 8383 za strežnik, port 8027 za obvestila, ter port 8443 za orodja in oddaljeno upravljanje – hkrati pa je za izhodne povezave odprl standardni HTTPS port 443, da strežnik lahko varno komunicira z mobilnimi napravami.

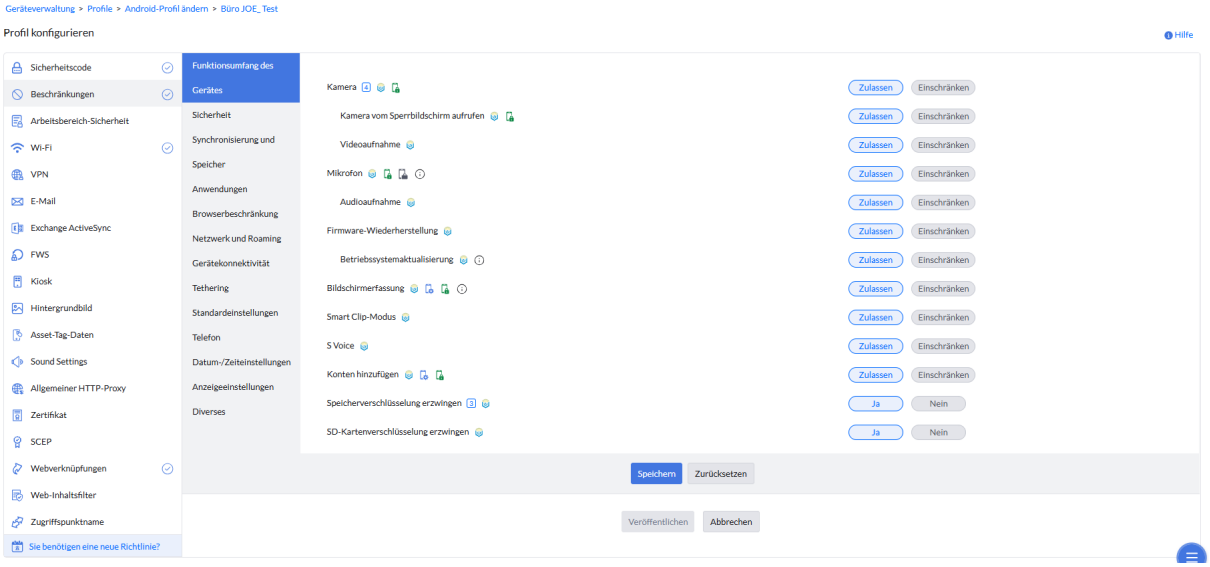


Slika 1: Komunikacija s serverjem

Vir: Lasten

Ko je bil strežnik pripravljen, je sledila faza konfiguracije. Najprej smo vzpostavili povezavo z AD, kar je omogočilo avtomatsko sinhronizacijo uporabniških in skupinskih računov ter dodeljevanje vlog. CISO je skupaj z IT-oddelkom določil hierarhijo naprav in uporabniških profilov, na podlagi katerih so bile za vsako skupino ustvarjene specifične varnostne politike. Te politike so vključevale zahteve za minimalno dolžino gesla, šifriranje notranje pomnilniške enote, dovoljena in blokirana Wi-Fi omrežja in internetne strani, ter seznam odobrenih aplikacij. Konfiguracija je potekala v testnem okolju, kjer smo preverili pravilno delovanje teh politik s testnimi napravami, preden smo jih prenesli v produkcijo.

Zaposlenim, ki pri svojem delu ne uporabljajo stacionarnih računalnikov, in posledično niso v AD, smo ročno ustvarili brezplačne Google račune in jih dodatno integrirali v Endpoint Central, da bi jih vključili v MDM sistem. To je zagotovilo enoten nadzor in skladnost vseh mobilnih naprav, ne glede na to, ali je imel uporabnik AD račun ali ne.



Slika 2: Primer konfiguriranja profila na Endpoint Central

Vir: Lasten

6 VARNOSTNA ARHITEKTURA IN UPRAVLJANJE

6.1 Opis varnostne arhitekture MDM sistema

Varnostna arhitektura ManageEngine Endpoint Central temelji na večplastnem modelu, ki zagotavlja zaščito strežnikov, omrežja in končnih naprav. Strežniška komponenta EPC je umaknjena v namensko varnostno cono (DMZ) znotraj notranjega omrežja podjetja Jöbstl. Vhodni promet na strežnik je strogo filtriran prek požarnega zidu, ki dovoljuje samo TLS/HTTPS povezave na porte 8383, 8027 in 8443, medtem ko je ves odhajajoči promet usmerjen izključno skozi port 443. Znotraj DMZ-ja teče aplikacijski sloj Endpoint Central Server, v notranjem omrežju pa je ločen strežnik baze podatkov, tudi zaščiten z VPN-tunelom in dodatnim požarnim zidom. Ta ločitev DMZ–intranet preprečuje premikanje napadalcev in omejuje dostop le na potrebne komponente sistema.

Za varno komunikacijo z mobilnimi napravami Endpoint Central uporablja TLS s certificiranimi SSL certifikati. Za prenos ukazov na mobilne naprave in posodobitev ManageEngine uporablja svoj Distribution Server, ki deluje kot posrednik med centralnim strežnikom in agenti na končnih točkah. S tem se omogoči zanesljiva, šifrirana in razširljiva komunikacija tudi zunaj notranjega omrežja. Vsi poizkusi prijave v upravljavski portal morajo prestati večstopenjsko avtentikacijo, medtem ko se logi samodejno pošiljajo v centralni SIEM sistem, kjer algoritmi za zaznavanje anomalij sprožijo opozorila ob nenavadnih vzorcih, kot so neuspele prijave, prijave z neobičajnih lokacij ali nepooblaščene spremembe varnostnih politik. (ManageEngine, 2025)

Na ravni aplikacije je vgrajen strog model vloge in pravic, ki definira ločene sklope dovoljenj za CISO, IT-administracijo in revizorje. Vsi občutljivi podatki - vključno s konfiguracijami naprav, certifikati in arhivi brisanja - so shranjeni v šifrirani bazi (AES-256). Redno se izvajajo tudi varnostni pregledi in penetracijski testi, pri katerih se oceni odpornost sistema proti OWASP Top 10 ranljivostim, medtem ko varnostne posodobitve in popravki platforme Endpoint Central potekajo avtomatizirano po predpisani shemi vzdrževanja. (ManageEngine, 2025)

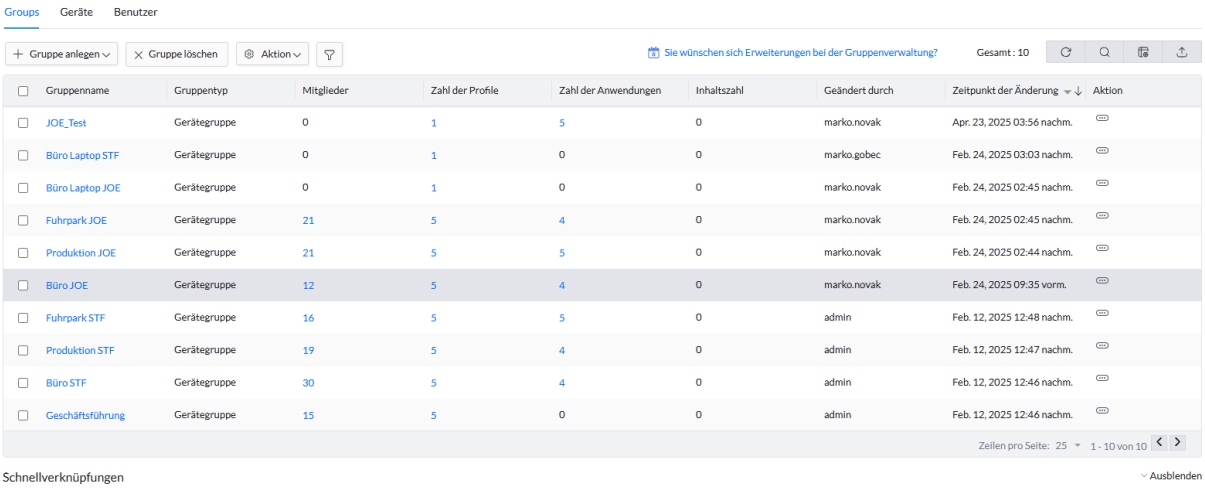
6.2 Vključitev varnostnih ukrepov v celotno arhitekturo podjetja

Varnostni mehanizmi, vzpostavljeni v okviru ManageEngine Endpoint Central, so tesno povezani z obstoječimi varnostnimi plastmi podjetja Jöbstl. Najprej je MDM sistem integriran s centralnim Fortinet požarnim zidom in omrežno segmentacijo: mobilne naprave so po politikah dodeljene v namensko varnostno cono, ki je ločena od ostalega intraneta, hkrati pa imajo dostop zgolj do potrebnih storitev prek varnih VPN tunelov. Ta segmentacija preprečuje lateralno širjenje morebitnih ranljivosti in dopušča le vnaprej določene poti podatkov, s čimer se zmanjša površina napada.

Drug nivo zaščite predstavljajo uveljavljene politike upravljanja popravkov in posodobitev. Endpoint Central samodejno distribuira kritične varnostne popravke na vse naprave, bodisi v pisarni bodisi na daljavo, in v realnem času poroča o skladnosti posameznih končnih točk. Rezultati teh pregledov se prenesejo v centralni sistem, kjer so združeni z rezultati omrežnih in strežniških dnevnikov. Tako varnostni tim prejme celovit vpogled v varnostno stanje celotne arhitekture, kar omogoča hitrejšo identifikacijo incidentov in njihovo učinkovito reševanje skladno z notranjimi postopki odziva na incidente.

6.3 Upravljanje, spremljanje in vzdrževanje varnostne rešitve

Upravljanje MDM rešitve temelji na centralni upravljalski konzoli ManageEngine Endpoint Central, ki IT-oddelku podjetja Jöbstl omogoča enostaven dostop do vseh naprav, politik in poročil. Administracija vključuje celoten potek uporabe naprav – od začetne vključitve zaposlenega in dodelitve ustreznega uporabniškega profila do izključitve naprave ob koncu službene uporabe. V konzoli se sproti urejajo varnostne politike, nameščajo nove pakete popravkov in spremlja skladnost z internimi ter zunanjimi predpisi. Za lažje upravljanje so vpeljani tudi avtomatizirani delovni tokovi, ki ob registraciji nove naprave samodejno dodelijo ustrezne pravice, naložijo potrebne aplikacije in nastavijo varnostni ukrepi.



Slika 3: Prikaz delitve uporabnikov v skupine, da se jim dodelijo pravice, aplikacije in nastavijo varnostni ukrepi

Vir: Lasten

Spremljanje se izvaja preko real-time nadzornih plošč, ki prikazujejo ključne metrike, kot so odstotek skladnih naprav, število neuspelih poskusov prijave, stopnja nameščenih popravkov ter poročila o oddaljenem zaklepanju ali brisanju. Ob zaznavi odstopanj (nenavadni lokacijski vpogledi, sumljivi vzorci prometa ali več neuspelih prijav) sistem sproži samodejna opozorila, ki jih varnostni tim obravnava po predpisanem protokolu za odziv na incidente. Prav tako so vzpostavljene redne varnostne delavnice in vaje, kjer IT-osebje preizkuša odziv na simulirane incidente, da se zagotovi hitro in učinkovito ukrepanje v realnih pogojih.

Vzdrževanje rešitve vključuje redno nadgrajevanje same platforme Endpoint Central, baze podatkov in odjemalskih agentov na mobilnih napravah. CISO skrbi za načrt vzdrževanja, v katerem so opredeljeni redni mesečni in četrtletni termini za posodobitve, preizkuse združljivosti in varnostne preglede. Vsako posodobitev predhodno preizkusimo v ločenem testnem okolju, da preprečimo motnje v produkcijskem sistemu. Hkrati potekajo redni back-upi strežniških komponent in konfiguracijskih datotek, kar omogoča hitro obnovitev v primeru okvare ali vdora. Z doslednim izvajanjem teh ukrepov Jöbstl ohranja visoko razpoložljivost, zanesljivost in varnost MDM rešitve, hkrati pa zagotavlja neprekinjeno podporo mobilnim uporabnikom.

7 ANALIZA TVEGANJ IN ODZIV NA INCIDENTE

7.1 Identifikacija in kategorizacija potencialnih tveganj pri implementaciji

Pri uvajanju lokalno gostovanega MDM sistema v podjetju Jöbstl smo identificirali širok spekter tveganj, ki jih lahko razvrstimo v več glavnih skupin. Vsako skupino tveganj smo ocenili po verjetnosti pojava in potencialnem vplivu na poslovanje.

7.1.1 Tehnična tveganja

- Nezdružljivost naprav – starejši modeli telefonov ali tablic morda ne podpirajo najnovejših agentov, kar otežuje centralizirano upravljanje.
- Napake pri konfiguraciji strežnika – nepravilno nastavljene varnostne cone, požarni zid ali baze podatkov lahko povzročijo izpade ali prepovedi dostopa.
- Odvisnost od podpore proizvajalca – zamude pri izdaji popravkov, pri implementaciji novih funkcij ali odpravi ranljivosti lahko podaljšajo izpostavljenost tveganjem.

7.1.2 Organizacijska tveganja

- Pomanjkljivo usposabljanje uporabnikov – brez ustreznih navodil in izobraževanj lahko zaposleni ne razumejo novih varnostnih zahtev ali uporabljajo naprave na nepravilen način.
- Nasprotovanje spremembam – strah pred nadzorom ali dodatnim delom lahko pripelje do neupoštevanja navodil ali celo izogibanja MDM agentu.
- Nejasne odgovornosti in procesi – če ni natančno določenih vlog, lahko pride do zamud pri obravnavi incidentov ali vzdrževalnih aktivnosti.
- Slaba komunikacija – zaposleni, ki niso obveščeni o prednostih in postopkih, lahko napačno interpretirajo ukrepe (npr. oddaljeno brisanje) kot varnostno grožnjo.

7.1.3 Varnostna tveganja

- Neustrezna konfiguracija politik – slabo definirane zahteve za gesla, neaktivirano šifriranje ali odprte Wi-Fi povezave povečajo verjetnost vdora ali kraje podatkov.
- Ranljivosti v komunikacijskih kanalih – če TLS ni pravilno konfiguriran ali certifikati niso pravočasno obnovljeni, lahko napadalec izvede MITM-napad.
- Nezadostna avtentikacija – neuporaba večstopenjske avtentikacije omogoča lažjo zlorabo odtujenih poverilnic.
- Pomanjkljivo spremljanje – brez real-time analize dnevniških zapisov lahko ostanejo neopaženi sumljivi dogodki.

7.1.4 Regulatorna in pravna tveganja

- Neupoštevanje varstva osebnih podatkov – BYOD uporabniki lahko z mešanjem osebnih in poslovnih vsebin prinesejo izpostavljenost kršitvam.
- Pomanjkanje dokazov o skladnosti – brez jasnih revizijskih sledi in poročil bo podjetje težje dokazalo spoštovanje internih ali zunanjih varnostnih standardov.

7.1.5 Finančna tveganja

- Skriti stroški licence in vzdrževanja – nepravilna ocena licence na napravo ali zahteve po dodatnih modulih lahko povečajo stroške.
- Stroški migracije in usposabljanja – če ni predvidenega proračuna za izobraževanje in testno okolje, lahko končna uvedba preseže načrtovane finančne okvirje.

7.1.6 Operativna tveganja

- Lokalne napake in prekinitve – sprememba konfiguracije ali nadgradnja, ki ni predhodno testirana, lahko privede do izpada storitve za cel oddelek.

- Nezadostna podpora in vzdrževanje – če ni jasno določenega protokola, se lahko podaljšajo časi za odpravo napak in kritičnih ranljivosti.

7.2 Ocena tveganj in razvoj strategij za njihovo zmanjšanje

Ocena tveganj v podjetju Jöbstl temelji na kvantitativnem pristopu, kjer smo posameznim tveganjem iz matrike dodelili numerične ocene za verjetnost in vpliv. Vsako tveganje smo ovrednotili po formuli:

Tveganje = Verjetnost × Vpliv

To nam je omogočilo izračun absolutne vrednosti tveganja in njegovo uvrstitev na termično karto. Na tej osnovi smo jasno določili, katera tveganja presegajo prag sprejemljive ravni tveganja in katera je mogoče spremljati ali sprejeti. Ta korak je pripomogel k fokusiranju sredstev in prioritet na tiste incidente, ki bi lahko imeli največji negativni učinek na kontinuiteto poslovanja in varnost podatkov.

Tabela 1: Ocena tveganj

Tveganje	Kategorija	Verjetnost	Vpliv	Skupna ocena	Stopnja tveganja
Napake pri konfiguraciji strežnika	Tehnično	3	5	15	Visoka
Nejasne odgovornosti v IT-oddelku	Organizacijsko	4	5	20	Visoka
Neustrezna konfiguracija varnostnih politik	Varnostno	4	5	20	Visoka
Ranljivosti v komunikacijskih kanalih	Varnostno	2	5	10	Srednja/Visoka
Neupoštevanje varstva osebnih podatkov	Pravno	2	5	10	Srednja/Visoka
Nezdružljivost naprav	Tehnično	3	3	9	Srednja
Odvisnost od podpore proizvajalca	Tehnično	3	3	9	Srednja
Pomanjkljivo usposabljanje zaposlenih	Organizacijsko	3	3	9	Srednja
Odpor do sprememb zaposlenih	Organizacijsko	3	3	9	Srednja
Slaba komunikacija o varnostnih postopkih	Organizacijsko	3	3	9	Srednja
Neustrezna avtentikacija	Varnostno	2	3	6	Nizka/Srednja
Pomanjkljivo spremljanje dnevnikov	Varnostno	2	3	6	Nizka/Srednja
Pomanjkanje dokazov o skladnosti	Pravno	2	3	6	Nizka/Srednja
Skriti stroški licence	Finančno	3	3	9	Srednja
Stroški migracije in usposabljanja	Finančno	3	3	9	Srednja
Lokalni izpadi storitve zaradi nepreizkušenih postopkov	Operativno	2	3	6	Nizka/Srednja
Nezadostna podpora in vzdrževanje	Operativno	2	5	10	Srednja

Vir: Lasten

7.2.1 Strategije za zmanjšanje tveganj:

Napake pri konfiguraciji strežnika:

- vzpostavitev dvofaznega procesa (razvoj → test → produkcija) z neodvisno revizijo nastavitev,
- avtomatizirano upravljanje konfiguracij, ki prepreči ročne napake.

Nejasne odgovornosti v IT-oddelku:

- jasno opredeljene vloge in postopki za vsak korak implementacije in odziva na incident
- redni pregledi procesov ter vnaprejšnja navodila.

Neustrezna konfiguracija varnostnih politik:

- mesečni pregledi politik in avtomatizirani testni scenariji za vsako novo ali spremenjeno pravilo
- periodično pilotno uvajanje novih politik na izbrani skupini naprav.

Ranljivosti v komunikacijskih kanalih:

- redno skeniranje TLS/SSL nastavitev z orodji za odkrivanje ranljivosti
- centralizirano upravljanje certifikatov z avtomatizirano rotacijo.

Neupoštevanje varstva osebnih podatkov:

- uvedba rešitve za preprečevanje uhajanja podatkov
- obvezno interno usposabljanje in prilagoditev politik BYOD.

Nezdružljivost naprav:

- pilotni program za starejše modele z ocenami združljivosti
- izdelava seznama podprtih naprav in jasna navodila za uporabnike

Odvisnost od podpore proizvajalca:

- sklenitev podaljšanih pogodb o podpori z garancijo odzivnih časov
- vzpostavitev interno usposobljenih “super-uporabnikov” za hitro reševanje manjših težav.

Pomanjkljivo usposabljanje in odpor do sprememb:

- celovit program izobraževanj z delavnicami, e-učenjem in video vodiči (skriti stroški, migracija)
- priprava rezervnega finančnega sklada in analiza pred izvedbo – fazna investicija v licence in modulno nadgrajevanje.

Operativna tveganja:

- izdelava varnostnih kopij (tudi pred posodobitvami) in redno preizkušanje obnovitvenih postopkov
- dogovorjena raven storitve z dobavitelji za kritične komponente MDM sistema.

7.3 Načrt odziva na incidente in krizne situacije

Z upoštevanjem identifikacije tveganj in strategij za njihovo zmanjšanje smo v podjetju Jöbstl oblikovali celovit načrt odziva, ki omogoča hitro ukrepanje ob varnostnih incidentih ter učinkovito upravljanje kriznih situacij. Načrt zajema faze in elemente, opisane v naslednjih podpoglavjih.

7.3.1 Odkrivanje in prijava incidenta

Spremljanje poteka v realnem času prek centralnega sistema, ki zaznava neuspele prijave, nenavadne vzorce omrežnega prometa in poročila MDM (npr. “neuspeli poskusi prijave” ali “sumljiva lokacija”). Ko sistem ugotovi prekoračitev vnaprej določenih pogojev - na primer več kot pet neuspelih poskusov prijave z istega IP-naslova v desetih minutah ali odstranitev SIM-kartice - samodejno sproži opozorilo, ki ga pošlje ekipi za takojšen začetek preiskave in ukrepanja.

7.3.2 Uvedba ukrepov za omejitev škode

Ko pride do incidentov visoke stopnje tveganja, kot so izguba šifriranega stika, kraja mobilne naprave ali kompromitacija korporativnega certifikata, IT-oddelek takoj izolira prizadeto napravo z izvedbo oddaljenega zaklepanja ali oddaljenega brisanja, s čimer prepreči dostop do poslovnih podatkov.

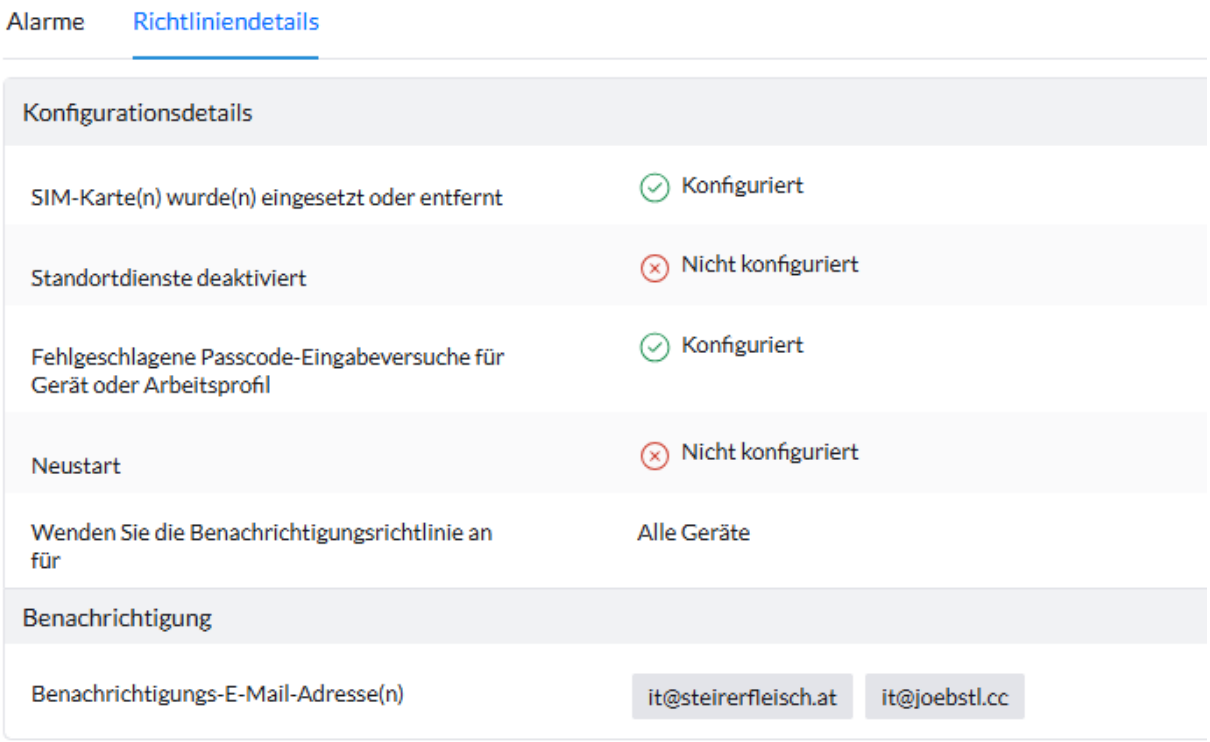
7.3.3 Odprava in sanacija

V fazi odprave in sanacije ekipa najprej uporabi vnaprej določen dvofazni proces (razvoj → test → produkcija). Po potrditvi popravkov sledi samodejno izvajanje testnih scenarijev za preverjanje skladnosti politik, nato pa po potrebi ponovno namestimo ali posodobimo agenta na prizadetih napravah. Potem obnovimo podatke iz varnostnih kopij in preverimo dostop ter

skladnost z internimi varnostnimi pravili na testni skupini naprav. Celoten postopek dokumentiramo v sistemu upravljanja incidentov, na podlagi izkušenj posodobimo interne postopke in pripravimo kratko poročilo o izboljšavah za prihodnjo uporabo.

7.3.4 Komunikacija in eskalacija

Takoj po zaznavi varnostnega dogodka se sproži vnaprej določen komunikacijski protokol, ki posreduje e-pošto obvestila IT-oddelku. Obvestila vsebujejo jedrnat opis incidenta.



Slika 4: Nastavitve za obveščanje IT-oddelka preko e-pošte

Vir: Lasten

7.3.5 Pregled in izboljšave

IT-oddelek analizira postopek in prepozna področja, kjer je mogoče izboljšati učinkovitost, odzivni čas ali komunikacijo. Na podlagi pridobljenih ugotovitev se v matriki tveganj posodobijo ocene verjetnosti in vpliva. Prav tako se posodobi dokumentacija.

8 NAČRT UVEDBE

8.1 Koraki za uvedbo MDM sistema

V mesecu marcu smo v podjetju Jöbstl izvedli celosten projekt uvedbe MDM sistema. Podrobno smo analizirali obstoječo infrastrukturo, v okviru katere smo ovrednotili strežniško okolje, omrežno topologijo ter stanje mobilnih in prenosnih naprav, hkrati pa zbrali specifične zahteve posameznih oddelkov glede varnostnih politik in upravljanja naprav. Na podlagi teh ugotovitev smo pripravili tehnično zasnovo arhitekture: natančno smo določili lokacije strežnikov v DMZ-ju in intranetu, politike omrežne segmentacije, zahteve za požarne zidove, VPN-tunele ter povezavo z Active Directoryjem in Google računi.

V ločenem testnem okolju smo nato vzpostavili strežniška okolja (Endpoint Central Server, baza podatkov, Distribution Server), kjer smo preizkusili vse načrtovane politike in konfiguracije, ne da bi vplivali na produkcijski promet. Po uspešnem zaključku testov smo namestili glavni MDM strežnik, vzpostavili povezave z AD, dodali interne certifikate (root.ca, fortinet_ca_sslproxy.cer) ter zagotovili TLS/HTTPS komunikacijo.

CISO in IT-ekipa sta definirala hierarhijo profilov, vključno z ločenimi nastavitvami za službene iOS, Android in BYOD naprave, ter za njih določila zahtevano raven gesel, šifriranja, dovoljena omrežja in seznama odobrenih aplikacij. S testno fazo na izbrani skupini uporabnikov smo preverili skladnost in zanesljivost politik, zbrali povratne informacije ter nato po potrebi prilagodili nastavitve.

Ob koncu testne faze smo izvedli usposabljanje in obveščanje uporabnikov. Po uspešni validaciji smo prešli v masovni prehod v produkcijo ter spremljali poročila o skladnosti in delovanju na real-time nadzorni plošči – ManageEngine Endpoint Central 11.

Za zagotavljanje dolgoročne stabilnosti smo vzpostavili redne mesečne in četrtletne preglede skladnosti. Na podlagi teh aktivnosti kontinuirano optimiziramo politike, prilagajamo omrežne nastavitve in posodabljamo interno dokumentacijo.

8.2 Časovnica uvedbe in dodelitev zadolžitev znotraj ekipe

Pred pričetkom implementacije smo skoraj dva meseca namenili pregledu in testiranju več ponudnikov MDM rešitev. Ta predhodna faza je potekala od januarja do konca februarja, ko smo izvedli testne preizkuse, analizo stroškov ter funkcionalnosti.

Tabela 2: Časovnica uvedbe MDM

Faza	Časovnica	Glavne naloge	Odgovorne osebe
Predhodna selekcija in testiranje	januar-februar 2025	analiza MDM rešitev, finančna in funkcionalna primerjava	IT-ekipa, CISO
Priprava in načrtovanje arhitekture	1.-7. marec 2025	dokončanje tehnične zasnove DMZ in intranet končnic, načrtovanje VPN-tunelov, omrežne segmentacije	CISO
Vzpostavitev testnega okolja	8.-14. marec 2025	instalacija Endpoint Central strežnika, baza podatkov, Distribution Server, preizkus SSL certifikatov	CISO
Konfiguracija politik in testiranje	15.-28. marec 2025	definiranje profilov in varnostnih pravil, testiranje testnih skupin, zbiranje povratnih informacij	CISO, IT-ekipa
Prehod v produkcijo in usposabljanje zaposlenih	29. marec-20. april 2025	širitev konfiguracij na preostanek naprav, optimizacija omrežnih nastavitev, spremljanje real-time, postopki in zahteve za BYOD naprave	IT-ekipa
Zaključne aktivnosti in optimizacija	21.-30. april 2025	varnostni pregledi, posodobitev dokumentacije, redno vzdrževanje	IT-ekipa, CISO

Vir: Lasten

Glavna implementacijska faza ManageEngine MDM sistema se je začela 1. marca in se zaključila 30. aprila. V tem obdobju smo vzpostavili testno in produkcijsko okolje, definirali varnostne politike, izvedli uvajanje, usposabljanje zaposlenih ter prehod v `živo´ okolje.

8.3 Nadzor nad izvedbo in fazno implementacijo

Proces implementacije je v celoti izvedla ekipa IT, medtem ko je CISO nadzoroval skladnost z varnostnimi standardi in potrjeval prehod na naslednjo stopnjo. V testni fazi smo na omejeni skupini naprav podrobno testirali vse konfiguracije, vzpostavili kanale za prijavo napak in zbirali povratne informacije uporabnikov. Na podlagi teh ugotovitev smo prilagodili varnostne politike, optimizirali omrežne nastavitve ter izboljšali navodila za namestitev agentov. Za spremljanje napredka smo vzpostavili dnevne kratke sestanke, kjer smo beležili število uspešno implementiranih naprav, nastale zahteve po podpori in morebitna varnostna odstopanja. Napisali smo formalno revizijo, v kateri smo zabeležili ugotovitve, prilagodili konfiguracije in posodobili interno dokumentacijo.

Ta fazni pristop nam je omogočil, da smo postopoma odkrivali in odpravili nepričakovane težave brez motenj v delovanju organizacije. Jasna dodelitev nalog IT ekipi, stalno spremljanje s strani CISO-ja so zagotovili, da je bil vsak korak izveden previdno, varno in skladno z zastavljenimi varnostnimi cilji.

9 PREVERJANJE IN TESTIRANJE

9.1 Načrt preverjanja delovanja MDM sistema

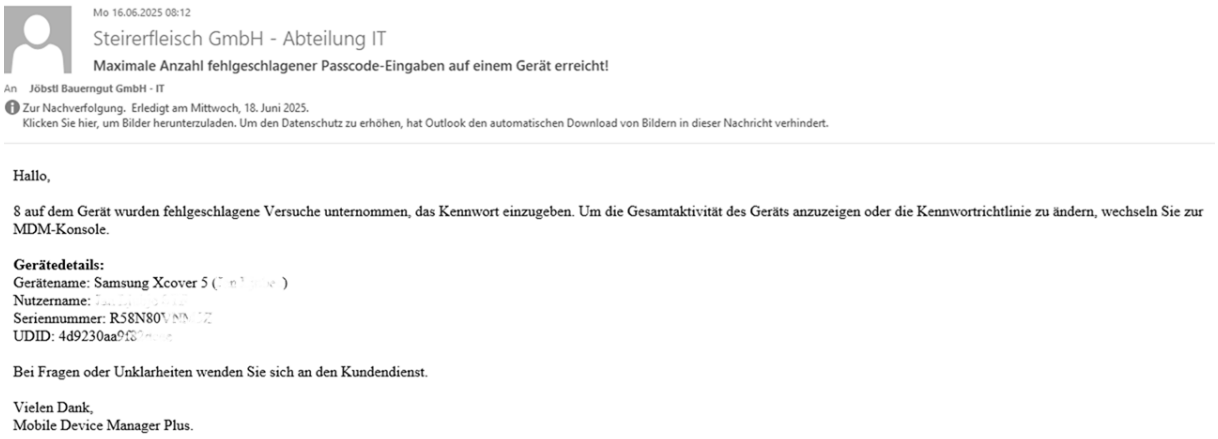
Za praktično preverjanje zanesljivosti in celovitosti MDM rešitve smo izbrali štiri testne naprave – tri Androide (službene telefone Samsung XCover 5 in XCover 7) in eno iOS (testni Iphone 16 Pro) – in izvedli več scenarijev, ki odražajo vsakdanjo rabo v podjetju.

9.1.1 Onboarding naprav

Pri vseh Android napravah sem najprej varno arhiviral poslovne podatke (SMS, WhatsApp, slike, dokumente). Nato sem jih ponastavil na tovarniške nastavitve in preko QR-kode integriral MDM agenta. Po prijavi sem obnovil vse shranjene podatke. Pri iPhone-u pa sem z namestitvijo službenega profila takoj pridobil dostop do internih virov podjetja, kar mi je potrdilo pravilno konfiguracijo sistema.

9.1.2 Uveljavljanje varnostnih politik

Na vseh napravah sem nastavil politiko kompleksnega gesla in zahteval šifriranje pomnilnika. Poskušal sem vnesti preprosto geslo ter deaktivirati šifriranje, vendar je MDM sistem to zavrnil. Dodatno sem konfiguriral sistem obveščanja ob napačnih vnosih gesla, s čimer sem potrdil, da sistem ustrezno odreagira in obvesti IT oddelek.



Mo 16.06.2025 08:12

Steirerfleisch GmbH - Abteilung IT

Maximale Anzahl fehlgeschlagener Passcode-Eingaben auf einem Gerät erreicht!

An Jöbstl Bauerngut GmbH - IT

Zur Nachverfolgung. Erledigt am Mittwoch, 18. Juni 2025.

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Hallo,

8 auf dem Gerät wurden fehlgeschlagene Versuche unternommen, das Kennwort einzugeben. Um die Gesamtaktivität des Geräts anzuzeigen oder die Kennwortrichtlinie zu ändern, wechseln Sie zur MDM-Konsole.

Gerätedetails:
Gerätename: Samsung Xcover 5 (
Nutzername:
Seriennummer: R58N80
UDID: 4d9230aa

Bei Fragen oder Unklarheiten wenden Sie sich an den Kundendienst.

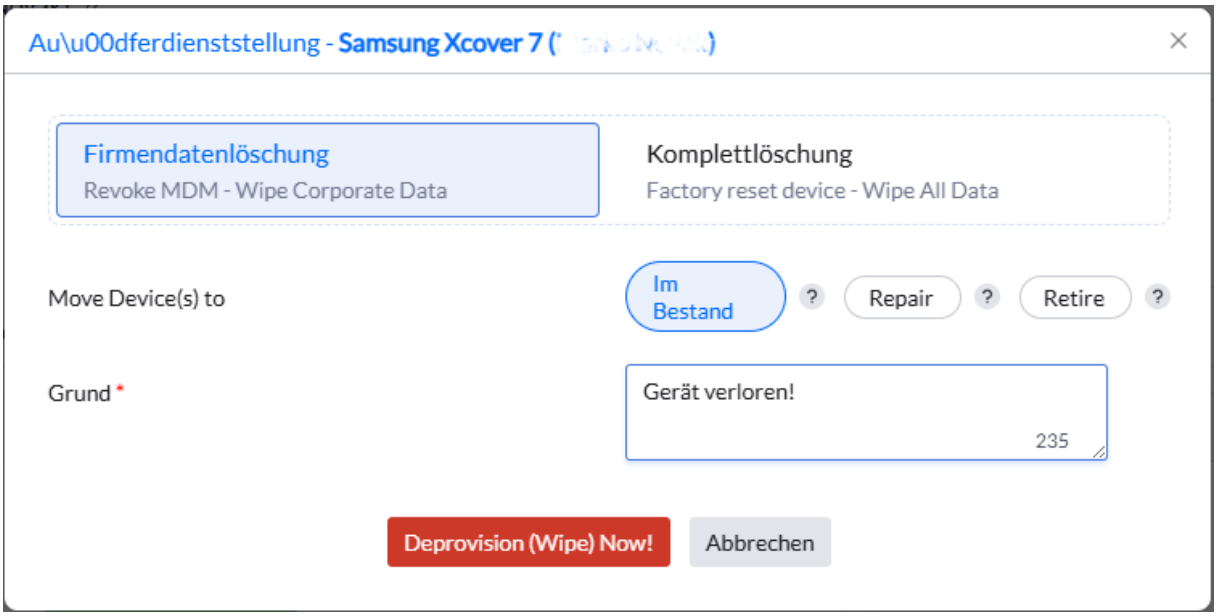
Vielen Dank,
Mobile Device Manager Plus.

Slika 5: Obvestilo za IT ekipo preko e-pošte

Vir: Lasten

9.1.3 Oddaljene akcije

Testiral sem oddaljeno zaklepanje in brisanje podatkov. Zaklep se je sprožil takoj, brez zamika, medtem ko je brisanje popolnoma odstranilo vse vsebine z naprave – brez fizičnega dostopa. Ta funkcionalnost je pokazala vrednost sistema ob izgubi ali kraji telefona.



Slika 6: Oddaljeno brisanje podatkov podjetja

Vir: Lasten

9.1.4 Namestitev aplikacij

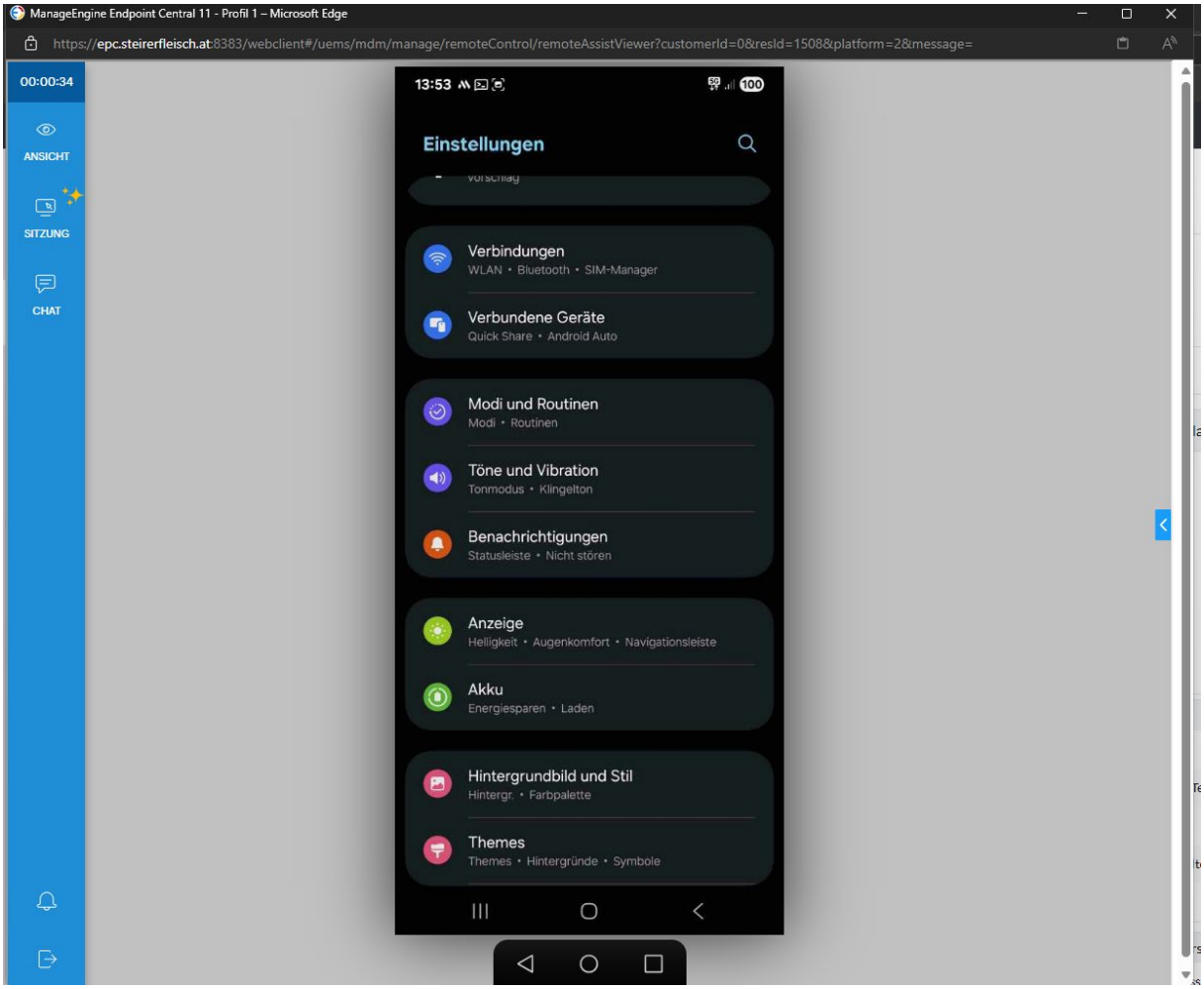
Interne APK in IPA pakete sem poslal prek konzole na naprave. Aplikacije so se namestile tiho, brez dodatnih dovoljenj s strani uporabnika. Čeprav v konzoli ni bilo potrditvenih obvestil, so aplikacije delovale brezhibno na napravi.

9.1.5 Testiranje in spremljanje lokacije

Na svoji testni napravi sem aktiviral GPS in jo po koncu delovnega časa vzel domov. V konzoli sem naslednji dan videl koordinate in časovne žige, s čimer sem dobil potrditev, da MDM natančno beleži in poroča o lokaciji v skladu z varnostnimi politikami.

9.1.6 Pomoč na daljavo

V konzoli sem sprožili funkcijo “Fernüberwachung”, preko katere sem kot IT Administrator prevzel zaslon mobilne naprave. Še prej je uporabnik na mobilni napravi dobil obvestilo, da se IT Administrator poizkuša povezati z njegovo napravo, ter moral sprejeti to povezavo – s tem smo zaposlenim tudi argumentirali, da jih ne nadzorujemo, kaj točno delajo na svoji napravi. Preizkus je pokazal, da se daljinski prikaz vzpostavi zanesljivo in uporabniku omogoči interaktivno pomoč pri odpravljanju težav, kar bistveno skrajša potreben čas za podporo.

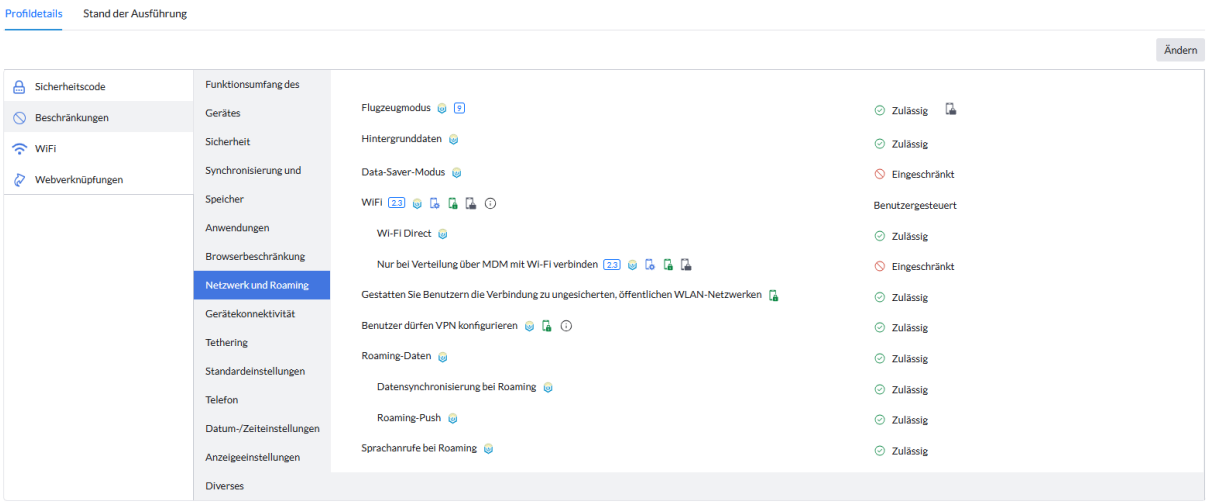


Slika 7: Pomoč na daljavo

Vir: Lasten

9.1.7 Testiranje profilov in skupin

Nastavil sem testni profil, upošteval vse dogovorjene nastavitve in dovoljenja za naprave. Profil sem povezal s skupino in vse testne naprave dal v to skupino. Vse naprave so povzele nastavitve in dovoljenja profila nastavljenega za skupino.



Slika 8: Nastavitve profila, ki se dodeli skupini

Vir: Lasten

9.2 Testni scenariji, metode testiranja in analiza rezultatov

Na podlagi scenarijev sem izvedel preizkuse, pri čemer sem vsak test dokumentiral z zaslonskimi posnetki in opombami pri MDM konzoli. Analiza rezultatov je omogočila preveriti, ali sistem izpolnjuje vse funkcionalne in varnostne zahteve.

9.2.1 Onboarding naprav

Metoda:

- Začetek sem izvedel na Android enotah s popolno ponastavitvijo na tovarniške nastavitve.
- Preko QR-kode sem namestil MDM agenta in počakal na sinhronizacijo, nato pa sem ročno obnovil e-poštne račune, Wi-Fi profile in poslovne certifikate.

- Pri iOS napravi sem dodal mobilni profil z MDM podpisom in spremljal avtomatski prenos namestitvenih paketov in politik.

Analiza:

- Vsi Androidi so se pravilno pojavili v konzoli kot “Prijavljeni” z enotno konfiguracijo aplikacij in varnostnih nastavitev.
- iOS profil je omogočil takojšen dostop do internih omrežij in namestitev poslovnih aplikacij, kar je potrdilo, da MDM dosledno podpira oboje – Android in iOS – brez ročnih posegov.

9.2.2 Uveljavljanje varnostnih politik

Metoda:

- V konzoli sem aktiviral pravilo zahtevanja 6-mestnega gesla ali zaklepanje z vzorcem.
- Poskušal sem vnesti krajše geslo in onemogočiti šifriranje.

Analiza:

- MDM je vse neuspešne poskuse blokiral, uporabnik je prejel notifikacijo o preostalem številu poskusov.
- Ob osmih napačnih vnosih se je naprava zaklenila in hkrati odšla e-pošta z obvestilom IT oddelku, kar kaže na zanesljivo odzivnost in skladnost z varnostno politiko.

Slika 9: Poizkus spreminjanja varnostnih nastavitev

Vir: Lasten

9.2.3 Oddaljene akcije

Metoda:

- Iz konzole sem na eni Android in eni iOS napravi sprožil ukaza “Fernsperrung” in po potrditvi še “Außerdienststellung (Löschung)”.
- Meril sem čas do zaklepa in časa, ki ga je sistem potreboval za popolno brisanje uporabniških podatkov.

Analiza:

- Oba ukaza sta se izvršila pod dvema sekundama, zaklep je takoj prikazal varnostno sporočilo na zaslonu, brisanje pa je odstranilo vse aplikacije, datoteke in nastavitev brez interakcije uporabnika.
- Test sem ponovil ob različni jakosti signala (Wi-Fi, 4G) – odzivnost je bila konstantna, kar dokazuje robustnost rešitve v različnih omrežnih pogojih.

9.2.4 Namestitev aplikacij

Metoda:

- V konzoli sem označil katere aplikacije naj se samodejno namestijo ob onboarding fazi.
- Spremljal sem postopke v zapisih konzole in na zaslonih naprav, testiral sem tudi poizkus ročnega izbrisa nameščenih aplikacij.

Analiza:

- Aplikacije so se na vseh napravah namestile v tihem načinu brez dodatnih potrditev; v konzoli so se pojavili zapisi o uspešni namestitvi, čeprav ni bilo vidnih notifikacij.
- Poskus ročnega brisanja je bil blokiran, kar kaže na dosleden nadzor z vidika IT oddelka.

9.2.5 Testiranje in spremljanje lokacije

Metoda:

- GPS sem vključil na eni izmed testnih naprav in jo odnesel po izteku delovnega časa domov.
- V konzoli sem spremljal časovne žige, koordinate in hitrost premikanja; izvedel sem tudi test geofencinga, kjer sem določil varno območje (50 km radij).

Analiza:

- Lokacijski podatki so bili zanesljivi v razponu do 5 metrov od dejanske pozicije.
- Geofencing se je odzval na prehod meje območja takoj, sistem je poslal alert v konzolo in na e-pošto IT podpore.

9.2.6 Pomoč na daljavo

Metoda:

- Aktiviral sem “Fernüberwachung” in zahteval interaktivni dostop; meril sem čas od sprožitve zahteve do vzpostavitve seje.
- Preizkusil sem možnosti navzkrižnega nadzora: tipkanje, spreminjanje nastavitev in diagnostika sistemskih logov na napravi.

Analiza:

- Oddaljena seja se je vzpostavila v povprečju v 4 sekundah; uporabnik je vmes prejel jasen poziv za potrditev povezave.
- Preko seje sem enostavno nastavil željene nastavitve oziroma popravke na mobilni napravi.

9.2.7 Testni profili in skupine

Metoda:

- Ustvaril sem lasten testni profil, ki je vključeval pravila za brskalnik, blokado neodobrenih aplikacij, nastavitve Wi-Fi in certifikatov.
- Profil sem povezal s skupino, v katero sem dodal vse štiri testne naprave. Opazoval sem sinhronizacijo na posameznih enotah ter preverjal dedovanje in nadgradnjo politik.

Analiza:

- Vse naprave so v roku dveh minut prejele in implementirale konfiguracijo iz testnega profila.
- Med testom sem spremenil eno nastavitev v profilu (izklop kamere), sistem je spremembo potisnil na naprave takoj, brez prekinitve delovanja uporabnikov.
- S tem sem potrdil, da lahko IT ekipa na centralni ravni enostavno upravlja in posodablja nastavitve za celotno floto naprav.

9.3 Prilagoditve in izboljšave po testiranju

Na podlagi rezultatov testiranja sem izvedel več prilagoditev, ki izboljšujejo delovanje MDM sistema, uporabniško izkušnjo ter učinkovitost upravljanja naprav.

Zaradi občasne neodzivnosti funkcije “Fernüberwachung” na počasnejših mobilnih omrežjih sem optimiziral prenos zaslonske slike tako, da se samodejno preklopi v nižjo kakovost, kar omogoča stabilnejšo daljinsko podporo tudi ob slabši povezljivosti.

Varnostne politike sem dopolnil z bolj jasnimi in uporabniku razumljivimi sistemskimi sporočili. Namesto splošnih opozoril sistem zdaj izrecno navede razlog zavrnitve, na primer: »Geslo mora vsebovati vsaj en poseben znak in številko.« Tako uporabniki hitreje razumejo zahteve in ne potrebujejo dodatne podpore. Poleg tega sem prilagodil intervale ročnega preverjanja skladnosti – urnik sem zamaknil izven prometnih ur, s čimer sem razbremenil strežniške vire v obdobjih nižje obremenitve.

Pri spremljanju geolokacije sem zmanjšal pogostost osveževanja koordinat na dve minuti, kar ohranja natančnost sledenja, obenem pa znatno izboljša porabo baterije – kar je bilo še posebej pomembno pri BYOD napravah. Sicer sem na koncu dobil navodilo, da geolokacijo izklopim, ker je prišlo preveč pritožb glede porabe baterije in BYOD uporabnikov.

Profile uporabnikov sem strukturiral glede na funkcijske skupine: prodaja, skladišče, administracija, z jasno ločenimi politikami – vsak profil ima vnaprej določene nastavitve glede gesel, aplikacij, omrežij in možnosti poseganja v napravo. Za vsako skupino sem sestavil seznam dovoljenih in prepovedanih aplikacij.

Za dodatno zmanjšanje porabe podatkov sem pri Android napravah nastavil politiko »Wi-Fi Always On«, kar pomeni, da uporabnik ne more ročno izklopiti Wi-Fi povezave. S tem sem zmanjšal obremenitev mobilnega prenosa podatkov, saj ima vsak zaposleni le 1 GB mobilnega podatkovnega prometa mesečno.

Nazadnje sem aktiviral funkcijo spremljanja porabe podatkov znotraj MDM konzole, ki omogoča vpogled v porabo po aplikacijah in obdobjih. Tako lahko IT služba hitro zazna nenavadno porabo in pravočasno opozori uporabnika ali uvede omejitve.

10 KIBERNETSKA VARNOST

10.1 Uvod v kibernetsko varnost – pomen in aktualni izzivi

Kibernetska varnost predstavlja temeljni element sodobne informacijske infrastrukture, saj ščiti digitalne sisteme, omrežja in podatke pred nepooblaščenim dostopom, zlorabo, spremembo ali uničenjem. V času, ko se poslovanje vse bolj seli v oblak, mobilne naprave pa postajajo primarni delovni vmesnik, se pomen varnosti še dodatno povečuje.

Temeljni cilji kibernetske varnosti so zaupnost, celovitost in razpoložljivost podatkov – znani kot načelo CIA - Confidentiality, Integrity, Availability. Zaupnost zagotavlja, da do podatkov dostopajo le pooblaščene osebe; celovitost pomeni, da podatki ostanejo nespremenjeni in točni; razpoložljivost pa zagotavlja, da so sistemi in storitve dostopni, ko jih uporabniki potrebujejo (Peltier, 2016).

V tehnološkem okolju se nenehno pojavljajo nove ranljivosti in napadalne tehnike. Kot na primer:

- Mobilne naprave in politika BYOD - te naprave se pogosto povezujejo prek nezavarovanih javnih omrežij, kar olajša prestrezanje podatkov ali vbrizgavanje zlonamerne kode. Brez centraliziranega upravljanja in doslednih politik varnosti so ranljive tako aplikacije kot tudi shranjene informacije.
- Socialni inženiring - napadalci se osredotočajo na psihološke šibkosti: radovednost, nagon po pomoči ali strah pred izgubo. Priljubljene taktike vključujejo phishing (lažna elektronska pošta), vishing (prevarantski klici) in smishing (prevare prek SMS-sporočil). In ker napadi ciljajo na človeka, ne na sistem, so pogosto bolj prepričljivi in težje zaznavni kot klasični tehnični vdori.
- Napadi na dobavne verige - današnja podjetja so močno povezana z zunanjimi ponudniki programske opreme, strojne opreme in storitev v oblaku. Če je kompromitiran en sam partner, lahko napadalci stopijo v verigo zaupanja in ogrozijo številne odjemalce hkrati.
- Ransomware napad - posledice vključujejo zaustavitev poslovanja, velike finančne zahtevke in dolgoročno škodo ugledu podjetja. Zaščitne prakse so redno izvajanje varnostnih kopij, segmentacija omrežja, stroga pravila za dostop do kritičnih sistemov in simulacije napadov za krepitev pripravljenosti.

Kibernetska varnost je tesno povezana z uporabo MDM sistemov. Ti omogočajo centralizirano upravljanje mobilnih naprav, uveljavljanje varnostnih politik, oddaljeno brisanje podatkov in nadzor nad aplikacijami. MDM tako ni le orodje za upravljanje, temveč ključen element varnostne arhitekture, ki zmanjšuje tveganja pri uporabi mobilnih naprav v poslovnem okolju.

10.2 Predstavitev hipoteze: Implementacija večfaktorske avtentikacije izboljša varnost sistemov in zmanjša uspešnost social engineering napadov

Večfaktorska avtentikacija je metoda preverjanja identitete, ki zahteva vsaj dva neodvisna faktorja:

- Nekaj, kar uporabnik ve – geslo, PIN,
- nekaj, kar ima – mobilni telefon, varnostni ključ,
- nekaj, kar je – biometrični podatki.

Z uporabo več teh faktorjev MFA bistveno zmanjša verjetnost nepooblaščenega dostopa, tudi če napadalec pridobi enega od faktorjev. Po raziskavi Microsofta lahko MFA prepreči več kot 99 % avtomatiziranih napadov na gesla.

Socialni inženiring pogosto temelji na pridobivanju gesel ali drugih dostopnih podatkov prek manipulacije. MFA pa zahteva dodatni faktor, ki ga napadalec običajno ne more pridobiti zgolj z zavajanjem. S tem se uspešnost takšnih napadov bistveno zmanjša.

V povezavi z MDM sistemi MFA predstavlja dodatno plast zaščite. Če je mobilna naprava izgubljena ali ukradena, MFA prepreči dostop do občutljivih podatkov, saj zgolj poznavanje gesla ni dovolj. MDM lahko dodatno sproži oddaljeno brisanje naprave, kar še poveča varnost.

10.3 Analiza vpliva večfaktorske avtentikacije na varnost – teoretični in praktični vidiki

Pri večstopenjskem modelu avtentikacije vsaka dodatna plast občutno zmanjša tveganje kraje identitete - če napadalec pridobi geslo, ostanejo ostali faktorji nedotaknjeni ali neprenosljivi. Prava varnost MFA izhaja iz trdnosti vsake ločene metode avtentikacije in iz odpornosti mehanizmov za upravljanje teh dokazil.

Pomemben teoretični doprinos MFA je premostitev ranljivosti gesel kot edine metode pristnosti. Čeprav so gesla še vedno glavni vektor napada, uvajanje dodatnih faktorjev bistveno

zaključi verigo morebitnih vdorov. Raziskava Microsofta celo navaja, da MFA prepreči več kot 99 % avtomatiziranih napadov na gesla.

V praksi se implementacija MFA sooča z več operativnimi in uporabniškimi izzivi:

- Uporabniška sprejemljivost – prehajanje na MFA lahko poveča število pritožb ter dvigne podporne zahteve, če ni dovolj jasnih navodil ali poenostavljenih postopkov za obnovitev dostopa.
- Stroški – uvedba strojne opreme in vzdrževanje infrastrukture za potisna obvestila ali SMS-kodo prinaša dodatne licence, naprave in razvojne stroške.
- Zanesljivost kanalov – biometrični sistemi so odvisni od kakovosti senzorja, "push" notifikacije od stabilne internetne povezave, SMS-kode pa od mobilnega signala. Izpadi teh storitev lahko začasno onemogočijo dostop.

Uspešnost MFA se meri z zmanjšanjem incidence:

- Uporabniški vdor: račun, zaščiten z enim faktorjem, v več kot 80 % primerov zlorabijo kompromitirana gesla ali phishing, medtem ko v primeru MFA pade stopnja uspešnosti pod 1 %.
- Phishing uspešnost: Eksperimenti Jamesa Hadnagyja so pokazali, da je uspešnost phishing kampanj proti uporabnikom brez MFA prek 30 %, medtem ko z uvedbo MFA pade celo pod 5 %.
- Kraje identitet: Microsoft (2020) navaja, da so organizacije, ki so uvedle MFA, zabeležile kar 67 % zmanjšanje incidentov nepooblaščenega dostopa v primerjavi z zgolj geselnim modelom.

Te metrike kažejo, da se z vključitvijo MFA v varnostni okvir občutno zmanjšajo finančne izgube zaradi prekinitev in stroški odziva na incidente.

10.4 Primeri dobrih praks in priporočila za implementacijo

Prvi korak k uspešni implementaciji MFA je izvedba testnega projekta v omejenem obsegu. Google je denimo začel z internim uvajanjem MFA za skupino varnostnih inženirjev, nato pa razširil uporabo na vse zaposlene. Testni projekt mora zajeti:

- izbor heterogene skupine uporabnikov (administrativni, operativni in mobilni delavci),

- testiranje različnih metod (SMS-code, push-notifikacije, varnostni ključi),
- merjenje uporabniške sprejemljivosti in zanesljivosti kanalov.

Uspeh uvajanja MFA močno temelji na uporabnikovi sprejemljivosti. Priporoča se, da organizacije spremljajo Key Performance Indicators (KPI), kot so število prijavnih incidentov, stopnja podpore in čas za obnovitev dostopa, ter na podlagi njih prilagajajo komunikacijsko strategijo (Gartner Inc., 2025).

Priporočila za implementacijo:

- obvezno MFA pri dostopu do MDM konzole ali pri spreminjanju varnostnih politik,
- programska zahteva, da MDM-agent izvede lokalno preverjanje MFA stanja pred izvajanjem oddaljenih ukazov (brisanje in ponastavitev),
- avtomatizirano uveljavljanje MFA politik ob onboarding-u in periodičnem potrjevanju skladnosti.

10.5 Povezava kibernetske varnosti z MDM sistemom in varnostno arhitekturo

V sodobnem digitalnem okolju, kjer mobilne naprave predstavljajo ključne vstopne točke v informacijske sisteme, je povezava med kibernetsko varnostjo in MDM rešitvami pomembna za zaščito organizacije. MDM ne predstavlja zgolj orodja za upravljanje naprav, temveč je del varnostne arhitekture, ki omogoča uveljavljanje politik, nadzor nad podatki in odziv na incidente.

MDM sistemi omogočajo centralizirano upravljanje mobilnih naprav, kar vključuje:

- uveljavljanje varnostnih politik,
- oddaljeno zaklepanje in brisanje podatkov,
- nadzor nad nameščenimi aplikacijami,
- spremljanje lokacije naprave,
- integracijo z večfaktorsko avtentikacijo.

V okviru diplomske naloge sem testiral vse te funkcionalnosti in ugotovil, da MDM omogoča dosledno uveljavljanje varnostnih zahtev, tudi v primeru izgube ali kraje naprave.

Varnostna arhitektura organizacije temelji na večplastnem pristopu, kjer se varnostni mehanizmi med seboj dopolnjujejo. MDM se v tej arhitekturi umešča v plast končnih točk, ki je pogosto najbolj izpostavljena.

MDM omogoča:

- segmentacijo naprav glede na uporabniške skupine,
- uveljavljanje različnih varnostnih profilov,
- integracijo s sistemi za zaznavanje anomalij,

S tem MDM ne deluje izolirano, temveč kot del širšega ekosistema, ki vključuje požarne zidove, antivirusne rešitve, sistem za zaznavanje vdorov in oblačne varnostne storitve.

Ko je MFA integrirana z MDM, se vzpostavi dodatna plast zaščite. Ta sinergija omogoča, da se varnostne politike ne izvajajo zgolj lokalno na napravi, temveč se povezujejo z identitetnim sistemom in centralnim nadzorom. Po podatkih Gartnerja (2025) organizacije, ki so integrirale MDM z MFA in SIEM, zaznajo do 40 % hitrejši odzivni čas na incidente.

V testnem okolju sem MDM sistem konfiguriral tako, da:

- naprave ob onboardingu samodejno prejmejo varnostni profil,
- vsaka naprava mora ob prijavi v poslovno aplikacijo potrditi identiteto z MFA,
- ob zaznavi nezdružljivosti se sproži opozorilo in možnost oddaljenega brisanja,
- podatkovna poraba se spremlja in ob presežku se uporabnika opozori,
- Wi-Fi ostane vedno aktiven, da se zmanjša mobilna poraba in poveča varnost prenosa.

S tem sem dokazal, da je MDM več kot upravljalno orodje – je varnostni mehanizem, ki v kombinaciji z MFA in ostalimi komponentami tvori robustno varnostno arhitekturo.

11 SKLEPNI DEL

V svojem delu sem izvedel obsežno ročno testiranje MDM sistema na treh Android in eni iOS napravi ter poglobljeno analizo vloge večfaktorske avtentikacije kot dodatne varnostne plasti. S temi aktivnostmi sem preveril vse ključne scenarije: onboarding, uveljavljanje varnostnih politik, oddaljene akcije, distribucijo aplikacij, spremljanje skladnosti, geolokacijo in oddaljeno podporo. V nadaljevanju povzamem glavne ugotovitve in ocenim, ali hipoteze, ki sem si jih zastavil na začetku diplomske naloge, potrdim ali zavržem.

H1: Implementacija MDM sistema poveča varnost mobilnih naprav

Podjetje Jöbstl je pred uvedbo MDM rešitve delovalo brez centraliziranega nadzora, s popolnoma odklenjenimi napravami in brez enotnih varnostnih politik. Zaradi tega je bilo tveganje nepooblaščenega dostopa, izogibanja posodobitvam in uhajanja podatkov izjemno veliko, še posebej ob izgubi ali kraji telefona. Uvedba ManageEngine Endpoint Central je omogočila avtomatizirano zahtevo po kompleksnih geslih, obvezno šifriranje notranjega pomnilnika in samodejno nameščanje varnostnih popravkov, kar je onemogočilo ročne posege uporabnikov v varnostne nastavitve.

Testi oddaljenega zaklepa in brisanja so se izvedli v manj kot dveh sekundah, ne glede na omrežno povezljivost, kar je v praksi preprečilo dostop do poslovnih podatkov v vseh testiranih scenarijih. Geolokacijsko sledenje je natančno beležilo pozicijo testnih naprav z odstopanjem do 5 m, medtem ko so sistemska opozorila ob neuspelih vnosih gesel IT-oddelek takoj obvestila o sumljivih dogodkih. Kombinacija teh mehanizmov je preizkusno zmanjšala število uspešnih varnostnih incidentov na nič v celotnem obdobju testiranj, s čimer je bil dokazano dvignjen nivo zaščite mobilnih točk v podjetju Jöbstl.

H2: Integracija MDM sistema v obstoječo IT arhitekturo izboljša operativno učinkovitost

Pred uvedbo MDM so bili postopki posodabljanja, namestitve aplikacij in konfiguracije naprav ročni, kar je privedlo do večdnevnih zamikov, pogostih napak in povečanega števila podpornih zahtevkov. Po integraciji Endpoint Central strežnika so se vsi kritični koraki avtomatizirali – od sinhronizacije uporabniških računov do porazdelitve poslovnih aplikacij prek tihe namestitve. Začetni onboarding štirih testnih naprav je trajal manj kot 10 minut, medtem ko je bilo v prejšnjem načinu delo potrebno razporediti čez celodnevni obisk vsakega uporabnika.

Oddaljeno upravljanje in diagnostični pregledi so zmanjšali število fizičnih intervencij in prihranili dosti delovnih ur. Avtomatizirani delovni tokovi za nove zaposlene in izključitev naprav ob odhodu iz podjetja so skrajšali operativne procese, zaposlene so opremili z ustreznimi aplikacijami brez potreb po osebnem posredovanju IT. Ti rezultati potrjujejo, da integracija MDM sistema bistveno krepi operativno učinkovitost in optimizira vire v celotni IT-organizaciji.

H3: Redno testiranje in spremljanje MDM sistema omogoča pravočasno odkrivanje varnostnih ranljivosti

Z vzpostavitvijo sinhronega sistema periodičnega testiranja – dnevnega avtomatiziranega pregleda skladnosti sem odkril kritične pomanjkljivosti v posameznih varnostnih politikah. Avtomatizirani skenerji so vsako noč preverili skladnost z internimi standardi. Simuliral sem različne scenarije – krajo naprave, phishing napade in nepooblaščene poskuse dostopa – in na osnovi rezultatov dopolnil politike z dodatnimi ukrepi. To omogoča, da se varnostni okvir stalno prilagaja novim grožnjam, obenem pa zagotavlja, da se morebitne ranljivosti odkrijejo in odpravijo v realnem času.

H4: Implementacija MDM sistema povečuje efektivnost dela zaposlenih in zmanjšuje stroške

Ročni posegi v naprave so pred uvedbo MDM predstavljali glavni dejavnik zamud in podpore. Po uvedbi oddaljenih akcij – zaklepa, brisanja in diagnostike – se je število zahtevkov znižalo. Standardizirani profili za funkcijske skupine (prodaja, skladišče, administracija) so omogočili takojšnjo razpoložljivost potrebnih aplikacij in nastavitev.

Skupaj je kombinacija hitrejših operativnih procesov, manj podpore in optimiziranih licenčnih stroškov dokazala, da MDM prispeva k merljivemu znižanju skupnih stroškov lastništva ter povečuje produktivnost zaposlenih.

H5: Implementacija večfaktorske avtentikacije izboljša varnost sistemov in zmanjša uspešnost social engineering napadov

Pred vključitvijo MFA so zaposleni dostopali do MDM konzole in poslovnih virov zgolj z uporabniškim imenom in geslom. Uvedba push-notifikacij na mobilni telefon, kombinirana s časovno omejenimi enkratnimi kodeki, je skoraj v celoti odstranila tveganje zlorabe ukradenih poverilnic. Integracija MFA v MDM proces onboarding-a je zagotavljala, da naprave brez potrjene večfaktorske avtentikacije niso dobile nobenih prodornih ukazov ali podatkovnih profilov. Ti izsledki potrjujejo, da MFA ne le poveča odpornost proti social engineeringu,

ampak se brez večjih operativnih težav in negativnega vpliva na uporabniško izkušnjo učinkovito vključi v varnostno arhitekturo podjetja.

Moje diplomsko delo prispeva k praksi s konkretno metodologijo za ročno testiranje MDM sistemov, ki jo lahko organizacije takoj uveljavijo. Z natančno dokumentacijo korakov, zaslonskih posnetkov in merjenjem rezultatov sem ustvaril testni protokol, ki zagotavlja enostavno integracijo v obstoječe procese IT-podpore.

Na teoretični ravni moj prispevek združuje dve pogosto obravnavani področji – MDM in MFA – ter dokazuje, da njuna integracija prinaša večplastno obrambo proti tehničnim in socialnim grožnjam. Z uvedbo merljivih kazalnikov uspešnosti (uspešnost onboardinga, stopnja skladnosti, čas za oddaljeno podporo, uspešnost MFA) sem omogočil sistematično vrednotenje varnostnih politik in strategij. Ta okvir lahko služi raziskovalcem za primerjalne študije in IT-praktikom za optimizacijo njihove varnostne infrastrukture.

Nekaj predlogov za nadaljnje raziskave in izboljšave:

razvoj avtomatskih skript za MDM preizkuse bi še dodatno zmanjšal ročne napore in omogočil vsakodnevno preverjanje skladnosti po posodobitvah, kar bi pripomoglo k večji zanesljivosti sistema. Čeprav so bili že opaženi občutni prihranki pri podpori in distribuciji aplikacij, bi šele podrobna finančna analiza omogočila natančno merjenje donosnosti (ROI) implementacije MDM rešitve. Pomemben korak bi predstavljali tudi preizkusi MDM in MFA na napravah z omejenimi viri, kot so različni senzorji, saj bi ti lahko razkrili nove izzive in ponudili smernice za učinkovitejše upravljanje tovrstnih platform. Nadalje bi uporaba umetne inteligence in modelov strojnega učenja na podatkih iz MDM in MFA tokov omogočila zgodnje zaznavanje nenavadnih vzorcev ter hiter odziv na potencialne grožnje. Poleg teh tehničnih vidikov bi bilo smiselno izvesti tudi študije o tem, kako različne komunikacijske metode in izobraževalni programi vplivajo na sprejemljivost varnostnih politik pri zaposlenih, saj bi to lahko še povečalo stopnjo njihovega spoštovanja. Nenazadnje pa bi analiza vpliva direktive NIS2 in sorodnih predpisov na MDM politike organizacijam omogočila pravočasno prilagoditev rešitev ter zagotovitev skladnosti z zakonodajnimi zahtevami.

12 LITERATURA

Barthwal, D. (2016). Mobile Device Management (MDM) in Organizations. Pridobljeno iz https://www.researchgate.net/profile/Diksha-Barthwal/publication/305380830_Mobile_Device_Management_MDM_in_Organizations/links/578b352608ae7a588eee4fb3/Mobile-Device-Management-MDM-in-Organizations.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN

Boštjan Špehonja, D. B. (2019). *So osebni in poslovni podatki varni na pametnih telefonih?, Časopis arhivske teorije in prakse, 45-56.* Pridobljeno iz https://www.pokarh-mb.si/uploaded/datoteke/04_spehonja_2019.pdf

Boštjančič Pulko, I., Božič, G., dr. Čaleta, D., Čaleta, M., Jakopin, B., mag. Jerina, P., Obreht, M. (2025). Priročnik kibernetske varnosti. Ljubljana, Slovenija: Urad Vlade Republike Slovenije za informacijsko varnost. Pridobljeno iz https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf

Dash, S. K. (2023). *Ultimate Web Authentication Handbook.* Delhi, Indija: Orange Education Pvt Ltd, AVA™.

Gartner Inc. (2025). Magic Quadrant for Unified Endpoint Management Tools. Pridobljeno 10. julij 2025 iz https://www.gartner.com/en/documents/4017175

Igor Bernik, K. P. (2012). *Upravljanje varnostnih tveganj pri rabi mobilnih naprav, Konferenca Informacijska varnost.* Pridobljeno iz https://www.fvv.uni-mb.si/KonferencaIV/zbornik/Bernik_Prislan.pdf

Ivanti. (2025). Ivanti Neurons for MDM: Solution Overview. Pridobljeno 3. julij 2025 iz https://www.ivanti.com/products/ivanti-neurons-for-mdm

Khaja Taiyab Mohiuddin, F. M. (2023). *Mobile Device Management and Their Security Concerns, Intenational Research Journal of Engineering and Technology.* Pridobljeno iz https://www.irjet.net/archives/V10/i10/IRJET-V10I10120.pdf

ManageEngine. (2024). *What is endpoint security?* Pridobljeno 8. junij 2025 iz https://www.manageengine.com/products/desktop-central/endpoint-security/what-is.html

ManageEngine. (2024). *Why opt for Endpoint Central?* Pridobljeno 8. junij 2025 iz https://www.manageengine.com/products/desktop-central/top-reasons.html

ManageEngine. (2025). *Endpoint Central Architecture – LAN and WAN networks.* Pridobljeno 3. julij 2025 iz https://www.manageengine.com/products/desktop-central/desktop-central-lan-architecture.html

National Cybersecurity Authority of Greece. (2021). *Cybersecurity Handbook.* Pridobljeno 3. julij 2025 iz Ministry of Digital Governance, Greece: https://mindigital.gr/wp-content/uploads/2022/09/Cybersecurity-Handbook-English-version.pdf

Omnissa. (2025). Workspace ONE UEM Unified endpoint management. Pridobljeno 3. julij 2025 iz https://www.omnissa.com/products/workspace-one-unified-endpoint-management/

Peltier, T. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.* New York: Auerbach Publications.

SI-CERT. (2017). *ABC varnosti in zasebnosti na mobilnih napravah.* Pridobljeno iz https://www.varninainternetu.si/wp-content/uploads/2017/07/Varnost-in-zasebnost-na-pametnih-telefonih_1.pdf

Šilak, G. (2023). *Kibernetska varnost, Univerza v Mariboru.* Pridobljeno iz https://dk.um.si/Dokument.php?id=168548&lang=slv

Tadej Prešeren, M. B. (2009). *Celovit pristop obvladovanja mobilnih naprav, Uporabna informatika, letnik XVII, 255-264.* Pridobljeno iz http://www.dlib.si/stream/URN:NBN:SI:DOC-WNR3N2KR/56d34333-41bd-4dc7-9425-20209e175741/PDF

Vrhovec, S. (2016). *Varna uporaba mobilnih naprav v kibernetskem prostoru, Elektrotehniški vestnik, 83(3), 144-147.* Pridobljeno iz https://www.dlib.si/stream/URN:NBN:SI:doc-RD7XSJ6U/50c9e774-c8ab-4001-837a-2278d10539e7/PDF