

SIGURNOSNA ARHITEKTURA · INŽENJERSKA NAČELA

Sigurnost je inženjerski zahtjev.

Sigurnosna arhitektura i inženjerska načela za softver kritične važnosti u javnom sektoru.

ID DOKUMENTA	VERZIJA	KLASIFIKACIJA	VLASNIK DOKUMENTA	CIKLUS REVIZIJE	OBJAVLJENO
ITO-TRUST-SEC-001	1.0	JAVNO	Informacijska sigurnost	Godišnje	Listopad 2026.

Sigurnost nije funkcionalnost. To je način na koji razvijamo.

Državne institucije, organizacije javne sigurnosti i operatori kritičnih usluga sve se više oslanjaju na digitalne platforme za podršku procesima koji zahtijevaju visoku razinu dostupnosti, cjelovitosti, povjerljivosti i odgovornosti.

Za ITO sigurnost stoga nije dodatna funkcionalnost softvera. Ona je **inženjerski zahtjev** koji utječe na to kako se sustavi dizajniraju, razvijaju, integriraju, implementiraju i održavaju tijekom cijelog životnog ciklusa.

ITO razvija softverske platforme za okruženja u kojima informacije mogu biti operativno osjetljive, pristup mora biti strogo kontroliran, aktivnosti u sustavu moraju biti sljedive, a integracije često povezuju više institucionalnih informacijskih sustava i vanjskih izvora podataka.

ITO platforme dizajnirane su za rad unutar institucionalnih okvira upravljanja. Institucija korisnik određuje operativne politike, ovlaštene korisnike, prava pristupa, zakonite svrhe, zahtjeve za čuvanje podataka i druga pravila upravljanja u skladu s mjerodavnim propisima, internim procedurama i ugovornim aranžmanima.

ITO osigurava tehnologiju potrebnu za provedbu tih pravila unutar opsega implementiranog rješenja.

Ovaj whitepaper opisuje inženjerska načela, procese i sigurnosne kontrole koji čine temelj razvoja i implementacije ITO softvera. Namijenjen je tehničkim donositeljima odluka, stručnjacima za informacijsku sigurnost, organizacijama javnog sektora, partnerima i drugim dionicima koji procjenjuju ITO tehnologiju.

NAŠ PRISTUP SIGURNOSTI POČIVA NA ČETIRI NAČELA

01

Ugrađena sigurnost

Sigurnosni zahtjevi razmatraju se tijekom izrade arhitekture i razvoja sustava, a ne uvode se tek nakon izrade.

02

Najmanje ovlasti

Korisnici, servisi i komponente sustava trebaju dobiti samo ovlasti potrebne za obavljanje predviđenih funkcija.

03

Višeslojna zaštita

Sigurnost ne ovisi o jednoj kontroli. Koristi se više tehničkih i organizacijskih zaštitnih mjera na razinama aplikacije, identiteta, podataka, integracija i infrastrukture.

04

Odgovornost i sljedivost

Sigurnosno relevantne aktivnosti trebaju se bilježiti na način koji institucijama omogućuje razumijevanje načina na koji se pristupa sustavima i informacijama i kako se koriste.

SADRŽAJ

01	Sažetak	02
02	Upravljanje sigurnošću	04
03	Upravljanje sigurnosnim rizicima	05
04	Ugrađena sigurnost	06
05	Upravljanje identitetom i pristupom	08
06	Sigurnost podataka	10
07	Sigurnost API-ja i integracija	12
08	Revizijski trag i sljedivost	14
—	Arhitektura na jednom mjestu	15
09	Infrastruktura i implementacija	16
10	Životni ciklus sigurnog razvoja	18
11	Upravljanje ranjivostima	21
12	Operativna sigurnost i incidenti	22
13	Treće strane i lanac opskrbe	24
14	Model podijeljene odgovornosti	26
15	Kontinuitet poslovanja i otpornost	28
16	Standardi i certifikati	29
17	Sigurnosna transparentnost	31
18	Otkrivanje ranjivosti	32
19	Jamstva za korisnike	33
20	Zaključak	34

KONTROLA DOKUMENTA

ID DOKUMENTA

ITO-TRUST-SEC-001

VERZIJA

1.0

KLASIFIKACIJA

JAVNO

VLASNIK

Informacijska sigurnost

CIKLUS REVIZIJE

Godišnje

OBJAVLJENO

Listopad 2026.

Institucije definiraju pravila. ITO osigurava tehnologiju.

ITO osigurava tehnologiju potrebnu za provedbu institucionalnih pravila unutar opsega implementiranog rješenja. Sigurnost je podijeljena između pružatelja tehnologije, institucije korisnika, pružatelja infrastrukture i, gdje je primjenjivo, tehnoloških partnera trećih strana.

PRUŽATELJ TEHNOLOGIJE

ITO

Osigurava tehnologiju potrebnu za provedbu institucionalnih pravila upravljanja unutar opsega implementiranog rješenja.

INSTITUCIJA KORISNIK

Definira pravila

Operativne politike, ovlašteni korisnici, prava pristupa, zakonite svrhe, zahtjevi za čuvanje podataka i druga pravila upravljanja.

PRUŽATELJ INFRASTRUKTURE

Udomljuje okruženje

Odgovoran za infrastrukturu na kojoj je rješenje implementirano, u skladu s dogovorenim operativnim modelom.

GDJE JE PRIMJENJIVO

Partneri treće strane

Tehnološki partneri čije komponente ili usluge čine dio implementiranog rješenja.

Cjeloviti model podijeljene odgovornosti opisan je u poglavlju 14. Pravila upravljanja postavlja institucija korisnik u skladu s mjerodavnim propisima, internim procedurama i ugovornim aranžmanima. ITO platforme dizajnirane su za rad unutar tih institucionalnih okvira upravljanja.

INSTITUCIJA ODREĐUJE

- Operativne politike
- Ovlaštene korisnike i prava pristupa
- Zakonite svrhe obrade
- Zahtjeve za čuvanje podataka
- Druga pravila upravljanja prema mjerodavnim propisima i ugovorima

ITO OSIGURAVA

- Sigurnu softversku arhitekturu i inženjering
- Tehnologiju za provedbu institucionalnih pravila
- Sigurnosne kontrole unutar opsega implementiranog rješenja
- Održavanje i ažuriranja u skladu s dogovorenim operativnim modelom

OPSEG OVOG DOKUMENTA



Ovaj dokument opisuje ITO-ov pristup sigurnosti na razini organizacije i zajednička inženjerska načela.

Pojedini proizvodi i implementacije mogu primjenjivati različite sigurnosne kontrole ovisno o svojoj arhitekturi, infrastrukturi, operativnim zahtjevima i okruženju korisnika. Sigurnosna dokumentacija specifična za proizvod i implementaciju stoga može dopunjavati ovaj whitepaper.

Sigurnost kao odgovornost organizacije

Informacijska sigurnost zahtijeva više od tehničkih kontrola. Zahtijeva jasno definirane odgovornosti, dokumentirane procese, upravljanje rizicima, kontinuirano poboljšanje i odgovornost organizacije.

ITO integrira informacijsku sigurnost u svoje upravljačke i inženjerske procese kroz politike, procedure i tehničke prakse osmišljene za zaštitu povjerljivosti, cjelovitosti i dostupnosti informacija i sustava.

SIGURNOSNE ODGOVORNOSTI KROZ ŽIVOTNI CIKLUS SOFTVERA

01 Arhitektura i dizajn rješenja	02 Razvoj softvera	03 Infrastruktura i implementacija
04 Upravljanje pristupom	05 Integracije sustava	06 Upravljanje promjenama
07 Upravljanje ranjivostima	08 Upravljanje incidentima	09 Sigurnosne kopije i oporavak
10 Rizici dobavljača i tehnologije	11 Kontinuirani nadzor i poboljšanje	

Sigurnost se tretira kao **multidisciplinarna odgovornost**, a ne kao izolirana aktivnost koju obavlja isključivo sigurnosna funkcija.

Upravljanje informacijskom sigurnošću

ITO održava sustav upravljanja informacijskom sigurnošću (ISMS) osmišljen kao strukturirani okvir za upravljanje rizicima informacijske sigurnosti. Okvir podržava sustavnu identifikaciju i obradu rizika povezanih s ljudima, procesima, tehnologijom i informacijama.

ITO-ove prakse upravljanja informacijskom sigurnošću potkrijepljene su certifikatom ISO/IEC 27001, uz ostale neovisno certificirane sustave upravljanja navedene u nastavku.

VAŽEĆI CERTIFIKATI

ISO 9001 UPRAVLJANJE KVALITETOM	ISO/IEC 27001 UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI	ISO/IEC 27701 UPRAVLJANJE PRIVATNOSTI I INFORMACIJAMA	ISO 30301 UPRAVLJANJE INFORMACIJAMA
---	---	---	---



Sigurnosna dozvola • Ministarstvo sigurnosti Bosne i Hercegovine

ITO posjeduje sigurnosnu dozvolu koju je izdalo Ministarstvo sigurnosti BiH.

Kontrole razmjerne riziku

ITO primjenjuje pristup informacijskoj sigurnosti utemeljen na riziku. Sigurnosni zahtjevi mogu se znatno razlikovati ovisno o prirodi sustava, informacijama koje se obrađuju, korisnicima, okruženju implementacije, integracijama i operativnoj svrsi.

Zbog toga sigurnosne kontrole trebaju biti razmjerne utvrđenim rizicima, a ne primjenjivati se isključivo kao standardni tehnički kontrolni popis.

SIGURNOSNA RAZMATRANJA MOGU UKLJUČIVATI

01 Osjetljivost podataka
Priroda i osjetljivost informacija koje sustav obrađuje.

02 Skupine korisnika
Interni korisnici, administratori, terensko osoblje, građani, vanjske organizacije ili strojni identiteti.

03 Vanjska izloženost
Jesu li komponente javno dostupne, ograničene na instituciju ili implementirane u izoliranim okruženjima.

04 Integracije
Veze s državnim registrima, sustavima identiteta, platnim sustavima, senzorima, kamerama, uslugama trećih strana ili drugim vanjskim sustavima.

05 Operativna kritičnost
Moguće posljedice prekida usluge, gubitka podataka ili neovlaštenog pristupa.

06 Okruženje implementacije
Lokalna infrastruktura, državni ili privatni oblak, hibridna arhitektura ili druga kontrolirana okruženja.

07 Regulatorni zahtjevi
Mjerodavni propisi, ugovorni zahtjevi, institucionalne politike i sektorske obveze.

KAKO SE ODREĐUJE SIGURNOSNA ARHITEKTURA

ITO inženjerski zahtjevi

Zajednička sigurnosna načela i inženjerske prakse koje se primjenjuju u razvoju ITO softvera.



Profil rizika implementacije

Specifični podaci, korisnici, izloženost, integracije, kritičnost, okruženje i regulatorni kontekst svake implementacije.



Sigurnosna arhitektura

Rezultirajući skup kontrola za to konkretno rješenje i implementaciju.

Sigurnost kroz cijeli životni ciklus softvera

Sigurnosna razmatranja počinju prije početka razvoja.

Tijekom dizajna rješenja inženjerski timovi identificiraju relevantne tokove informacija, korisnike, integracije, granice povjerenja i sigurnosne zahtjeve koji mogu utjecati na arhitekturu rješenja.

TIPIČAN ŽIVOTNI CIKLUS



↻ Povratna informacija ulazi u zahtjeve za sljedeće izdanje

Sigurnost je dio svake faze, od utvrđivanja zahtjeva do dugoročnog rada, a ne korak koji se uvodi tek nakon izrade.

Višeslojna zaštita i sigurne zadane postavke

Višeslojna zaštita

ITO sustavi dizajnirani su prema načelu da nijedan pojedinačni sigurnosni mehanizam ne smije biti jedina zaštita od sigurnosne prijetnje.

Ovisno o rješenju i arhitekturi implementacije, sigurnosne kontrole stoga mogu postojati na više razina.

Kompromitacija ili zakazivanje jedne kontrole **ne bi smjelo automatski dovesti do neograničenog pristupa** cijelom sustavu.

Sigurne zadane postavke

Gdje je to tehnički i operativno prikladno, ITO sustavi dizajnirani su tako da sigurnosno osjetljive funkcionalnosti zahtijevaju izričitu konfiguraciju ili ovlaštenje, umjesto da su prema zadanim postavkama neograničene.

PRIMJERI MOGU UKLJUČIVATI

Ograničene administrativne funkcionalnosti

Ovlaсти temeljene na ulogama

Kontrolirane integracije sustava

Konfiguraciju specifičnu za okruženje

SIGURNOSNE RAZINE

Korisnici	ULAZ
Identitet i autentifikacija	01
Autorizacija i kontrola pristupa	02
Sigurnost aplikacije	03
Sigurnost API-ja i integracija	04
Zaštita podataka	05
Revizija i nadzor	06
Sigurnost infrastrukture i mreže	07
Operativna sigurnost	08

Detaljan prikaz. Prikazane razine su okvirne; kontrole primijenjene na svakoj razini ovise o rješenju i arhitekturi implementacije. Sažeti prikaz u šest razina nalazi se na stranici **Sigurnosna arhitektura na jednom mjestu**.

Kontrolirani pristup sustavima i informacijama

Upravljanje identitetom i pristupom temeljna je sigurnosna razina svih ITO platformi.

Pristup funkcionalnostima sustava i informacijama zasniva se na **autentificiranim identitetima, definiranim ulogama i izričitim ovlastima**. Cilj je osigurati da korisnici i komponente sustava mogu pristupiti samo resursima potrebnima za njihove ovlaštene odgovornosti.

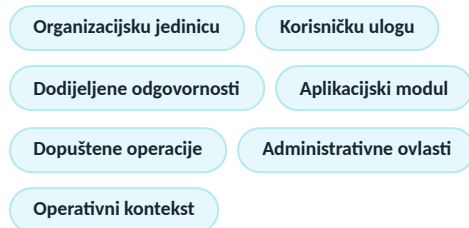
ITO rješenja dizajnirana su da podrže modele kontrole pristupa prilagođene organizacijskoj strukturi i operativnim zahtjevima institucije.



Kontrola pristupa temeljena na ulogama

ITO platforme mogu primjenjivati kontrolu pristupa temeljenu na ulogama (RBAC) kako bi ovlasti povezale s definiranim organizacijskim i operativnim ulogama.

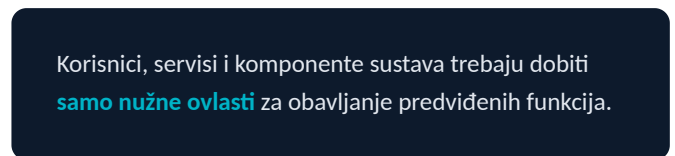
OVISNO O RJEŠENJU, POLITIKE PRISTUPA MOGU UZIMATI U OBZIR



To institucijama korisnicima omogućuje da organizacijske odgovornosti pretoče u provedive ovlasti na razini aplikacije.

Načelo najmanjih ovlasti

ITO primjenjuje načelo najmanjih ovlasti pri dizajnu mehanizama kontrole pristupa.



Administrativne i povlaštene funkcije trebaju biti odvojene od standardnih korisničkih operacija gdje god je to tehnički i operativno prikladno.

Autentifikacija, povlašteni pristup i životni ciklus pristupa

Autentifikacija i poslovni identitet

ITO rješenja podržavaju integraciju s institucionalnom infrastrukturom za upravljanje identitetima i standardnim mehanizmima autentifikacije.

PODRŽANI MEHANIZMI UKLJUČUJU

Active Directory / LDAP

Jedinstvena prijava (SSO)

Višefaktorska autentifikacija

Autentifikacija i autorizacija temeljene na standardima

Sve ITO platforme podržavaju ove mehanizme. Model koji se koristi u pojedinoj implementaciji odabire se prema okruženju implementacije i sigurnosnim zahtjevima korisnika.

Administrativni pristup

Administrativni pristup predstavlja veći sigurnosni rizik i stoga treba podlijegati strožim kontrolama.

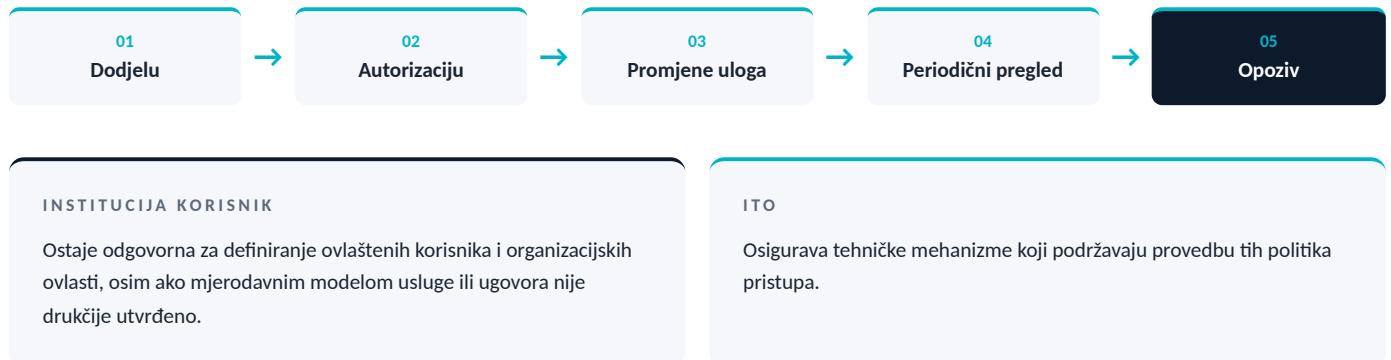
OVISNO O MODELU IMPLEMENTACIJE, KONTROLE MOGU UKLJUČIVATI

- Ograničene administrativne uloge
- Razdvajanje administrativnih odgovornosti
- Strože zahtjeve za autentifikaciju
- Kontrolirani pristup infrastrukturi
- Bilježenje sigurnosno relevantnih administrativnih aktivnosti

ITO preporučuje da povlašteni pristup bude ograničen na ovlašteno osoblje i da ga odgovorna organizacija periodično preispituje.

Životni ciklus pristupa

Sigurnost pristupa ne završava stvaranjem korisničkog računa. Životni ciklus identiteta treba obuhvatiti:



PODRŽANO NA SVIM ITO PLATFORMAMA

Poslovni identitet na svakoj platformi

✓ Active Directory / LDAP

✓ Jedinstvena prijava (SSO)

✓ Višefaktorska autentifikacija

✓ Lokalni identitet

✓ OAuth 2.0 / OpenID Connect

PLATFORME

Renata

Carmen

AssetIX

eVa

CollaBIZ

eCTZen

GOV-cms

Marina

AURA

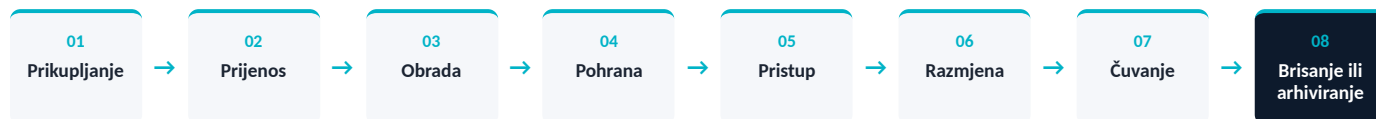
eAppointment

RIS WPR

Zaštita informacija kroz cijeli životni ciklus

ITO sustavi mogu obrađivati informacije različite razine osjetljivosti, od administrativnih evidencija do operativnih informacija koje koriste državne institucije i organizacije javne sigurnosti.

Zaštitu podataka stoga treba razmatrati kroz cijeli životni ciklus informacija.



Sigurnosne kontrole primijenjene u svakoj fazi ovise o vrsti informacija, arhitekturi sustava, okruženju implementacije, zahtjevima korisnika i mjerodavnom regulatornom okviru.

U PRIJENOSU

Podaci u prijenosu

Komunikacija između komponenti sustava i vanjskih servisa treba koristiti sigurne transportne mehanizme primjerene arhitekturi implementacije.

Gdje je primjenjivo, ITO rješenja koriste standardne šifrirane komunikacijske protokole poput **TLS-a** za zaštitu informacija koje se prenose mrežom.

Naslijeđene integracije ili integracije specifične za instituciju mogu zahtijevati drukčije mehanizme, koji se procjenjuju prema zahtjevima i mogućnostima povezanog sustava.

U MIROVANJU

Pohranjeni podaci

Zaštita pohranjenih informacija može se provoditi na različitim infrastrukturnim i aplikacijskim razinama, ovisno o implementiranom rješenju.

KONTROLE MOGU UKLJUČIVATI

Sigurnosne mehanizme baze podataka

Šifriranu pohranu

Kontrole operacijskog sustava

Šifriranje na razini infrastrukture

Zaštićenu pohranu sigurnosnih kopija

Točni mehanizmi ovise o infrastrukturi korisnika, tehnologiji baze podataka, arhitekturi implementacije i dogovorenim sigurnosnim zahtjevima.

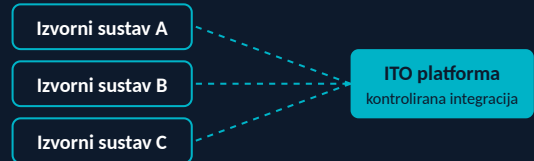
Minimizacija, čuvanje i oporavak

Minimizacija podataka

ITO podržava načelo da sustavi obrađuju informacije potrebne za njihovu definiranu operativnu svrhu. Arhitektura sustava treba izbjegavati nepotrebno umnožavanje, prikupljanje ili čuvanje informacija kada takva obrada nije potrebna zbog operativnih, pravnih ili tehničkih zahtjeva.

INTEGRACIJA BEZ CENTRALIZACIJE

Gdje je moguće, integracije mogu omogućiti da informacije ostanu u **izvornim (mjerodavnim) sustavima**, bez nepotrebnog repliciranja u dodatne baze podataka.



Čuvanje podataka

Zahtjevi za čuvanje podataka u pravilu se određuju mjerodavnim propisima, institucionalnim procedurama, operativnim zahtjevima i ugovornim aranžmanima.

ITO PLATFORME

Mogu pružati tehničke mogućnosti koje podržavaju politike čuvanja i životnog ciklusa.

ODGOVORNA INSTITUCIJA

Određuje primjenjiva pravila unutar svog pravnog i operativnog okvira.

Sigurnosne kopije i oporavak

Zahtjevi za sigurnosne kopije i oporavak ovise o kritičnosti rješenja i arhitekturi implementacije.

KADA SU UKLJUČENE U DOGOVORENI OPSEG, STRATEGIJE SIGURNOSNIH KOPIJA MOGU OBUHVATITI

Cjelovitost podataka

Učestalost izrade kopija

Čuvanje

Zaštitu pristupa

Procedure vraćanja

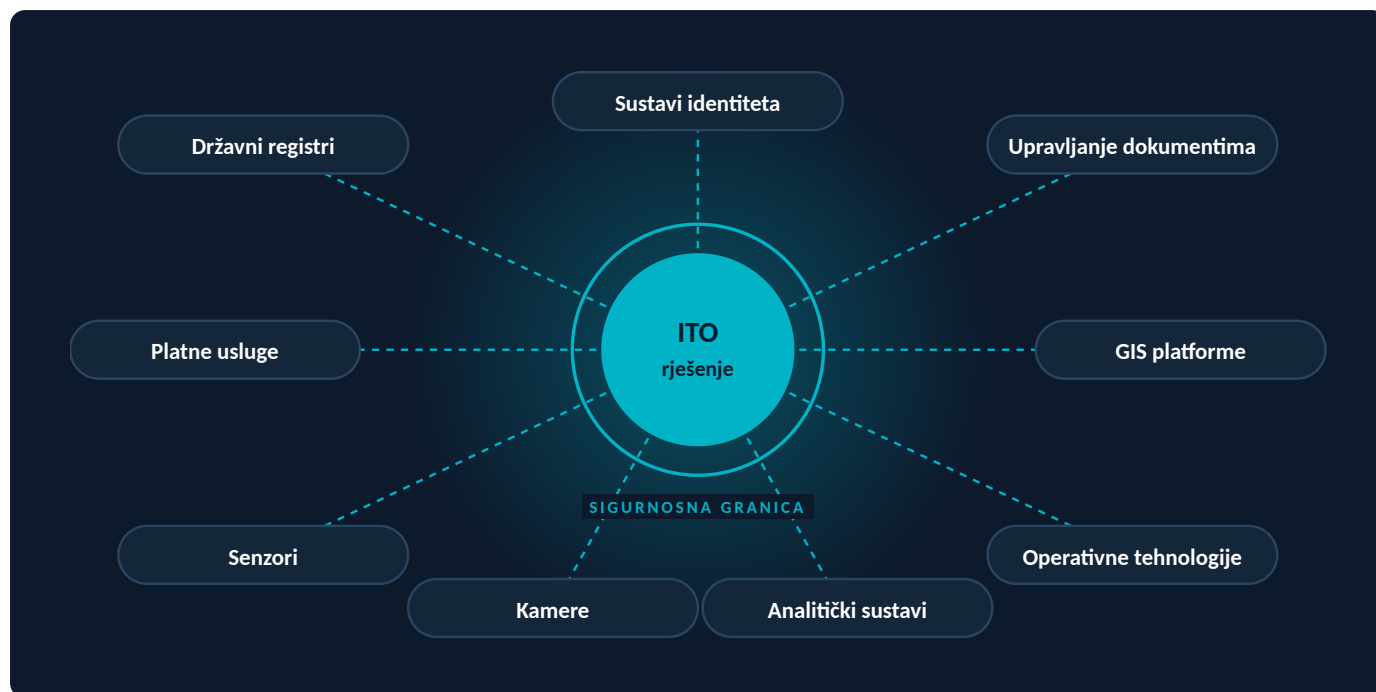
Ciljeve oporavka

Mehanizme sigurnosnih kopija treba periodično provjeravati odgovarajućim testiranjem vraćanja ili oporavka.

Sigurna interoperabilnost

Suvremene državne platforme rijetko rade samostalno. Svaka integracija stvara i operativnu vrijednost i potencijalnu sigurnosnu granicu.

Zbog toga interoperabilnost treba razvijati imajući na umu sigurnost.



Arhitektura integracija

ITO daje prednost kontroliranim i dokumentiranim sučeljima između sustava umjesto nekontroliranog izravnog pristupa aplikacijskim bazama podataka. Gdje je prikladno, integracije se izvode putem API-ja, web servisa, infrastrukture za razmjenu poruka ili drugih definiranih integracijskih mehanizama.

IZBJEGAVA SE

Nekontrolirani izravni pristup bazi podataka

Vanjski sustavi koji izravno čitaju ili pišu u aplikacijske baze podataka, bez definiranog sučelja.

PREFERIRA SE

Kontrolirana, dokumentirana sučelja

API-ji, web servisi, infrastruktura za razmjenu poruka ili drugi definirani integracijski mehanizmi koji osiguravaju jasnije razdvajanje sustava.

PRIMJENJUJE SE NA GRANICI INTEGRACIJE

Autentifikacija

Autorizacija

Validacija

Bilježenje

Upravljanje životnim ciklusom

Zaštita granice integracije

Sigurnost API-ja

Ovisno o arhitekturi integracije, sigurnosne kontrole API-ja mogu uključivati:

01	Autentificirani pristup API-ju	02	Autorizaciju API operacija	03	Komunikaciju zaštićenu TLS-om
04	Autentifikaciju temeljenu na tokenima	05	OAuth 2.0 ili srodne standarde, gdje je primjenjivo	06	Validaciju zahtjeva
07	Kontrolirane servisne račune	08	Bilježenje relevantnih integracijskih aktivnosti	09	Ograničenja učestalosti ili pristupa, gdje je potrebno

Vanjski sustavi

Sigurnost integracije ovisi o obje strane veze.

ITO može osigurati sigurne integracijske mogućnosti, ali ukupna sigurnost razmjene informacija može ovisiti i o arhitekturi, protokolima i kontrolama koje podržava vanjski sustav.

Kada su uključeni naslijeđeni sustavi ili tehnologije specifične za instituciju, mogu biti potrebne odgovarajuće kompenzacijske kontrole.

Integracijske vjerodajnice

Vjerodajnice, certifikate, tokene i druge tajne koje se koriste za komunikaciju između sustava treba zaštititi od neovlaštenog pristupa i nepotrebnog izlaganja.

Njihova pohrana, distribucija, rotacija i opoziv trebaju slijediti odgovarajuće sigurnosne procedure ovisno o implementiranoj arhitekturi.

Pohrana

Distribucija

Rotacija

Opoziv

INTEROPERABILNOST BEZ NEPOTREBNOG UMNOŽAVANJA PODATAKA

Povežite izvorne sustave. Nemojte ih kopirati.

ITO-ova filozofija integracije temelji se na povezivanju mjerodavnih izvora informacija, a ne na automatskom stvaranju dodatnih kopija institucionalnih podataka.

Kada operativni i tehnički zahtjevi to dopuštaju, sustavi mogu dohvaćati ili razmjenjivati potrebne informacije kontroliranim integracijama, dok mjerodavni podaci ostaju u odgovornom izvornom sustavu. To može smanjiti nepotrebno umnožavanje podataka i istovremeno podržati dosljedan pristup ažurnim informacijama.

Odgovornost kroz revizijski trag

U informacijskim sustavima kritične važnosti kontrola pristupa samo je dio sigurnosnog modela. Institucije mogu trebati razumjeti i:

Tko?

Tko je pristupio sustavu?

Što?

Koja je radnja izvršena?

Kada?

Kada se to dogodilo?

Koji?

Koji su sustav ili proces bili uključeni?

Revizijski trag podupire odgovornost, sigurnosne istrage, operativni nadzor i procese usklađenosti.

Revizijsko bilježenje

Ovisno o proizvodu i konfiguraciji implementacije, ITO rješenja mogu bilježiti sigurnosno relevantne i operativne događaje kao što su:

- Događaji autentifikacije
- Korisničke radnje
- Administrativne aktivnosti
- Promjene relevantnih zapisa
- Integracije sustava
- Odabrani događaji pristupa podacima
- Prijelazi u radnim tokovima
- Pogreške sustava i sigurnosno relevantni događaji

Točan opseg bilježenja ovisi o arhitekturi sustava, zahtjevima korisnika i mjerodavnim politikama upravljanja.

TEHNOLOGIJA OSIGURAVA

Dokaze potrebne za nadzor.

Zaštita revizijskih zapisa

Revizijske informacije i same trebaju biti zaštićene od neovlaštenog pristupa, izmjene i brisanja.

Pristup revizijskim informacijama stoga treba biti ograničen u skladu s odgovarajućim administrativnim i sigurnosnim odgovornostima.

Rok čuvanja revizijskih zapisa treba definirati u skladu s operativnim, ugovornim i mjerodavnim regulatornim zahtjevima.

Podrška institucionalnom nadzoru

Revizijske mogućnosti mogu ovlaštenom osoblju institucije omogućiti istraživanje aktivnosti, pregled korištenja sustava i rekonstrukciju relevantnog slijeda događaja.

INSTITUCIJA OSTAJE ODGOVORNA ZA

Definiranje procedura upravljanja i određivanje načina na koji se revizijske informacije pregledavaju i na temelju njih postupaju.

Koordinirane kontrole, s kraja na kraj

Sažeti prikaz kontrola opisanih u poglavljima 4–8, koji grupira detaljne razine višeslojne zaštite iz poglavlja 4.

INSTITUCIONALNO UPRAVLJANJE
Politike • Uloge • Procedure • Pravna osnova



01	Identitet i pristup	Autentifikacija • RBAC • Najmanje ovlasti
02	Sigurnost aplikacije	Autorizacija • Validacija • Sigurno kodiranje
03	Sigurnost integracija	API-ji • TLS • Autentifikacija • Validacija
04	Sigurnost podataka	Prijenos • Pohrana • Sigurnosne kopije • Životni ciklus
05	Revizijski trag i nadzor	Bilježenje • Sljedivost • Nadzor
06	Infrastruktura i rad sustava	Ojačavanje • Mreže • Nadzor • Oporavak

Sigurnost nije pojedinačna funkcionalnost proizvoda. To je skup koordiniranih kontrola koje obuhvaćaju upravljanje, identitet, aplikacije, integracije, podatke i infrastrukturu.

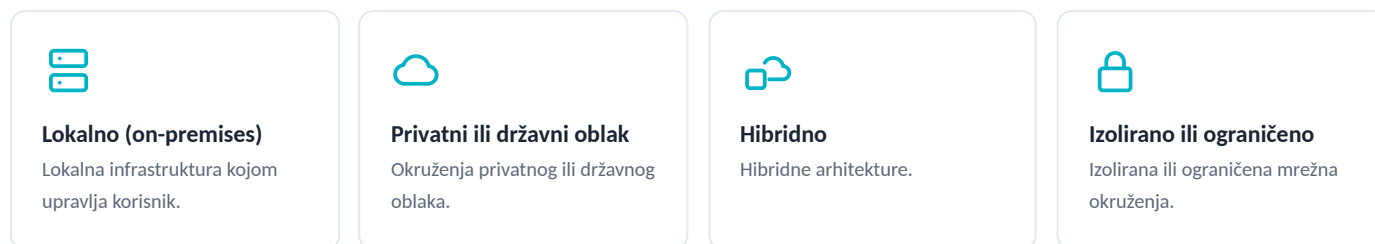
Sigurnost u različitim okruženjima implementacije

Državni sustavi i sustavi kritične važnosti mogu raditi na različitim infrastrukturnim modelima, ovisno o institucionalnim zahtjevima, regulatornim ograničenjima, postojećem tehnološkom okruženju i operativnim potrebama.

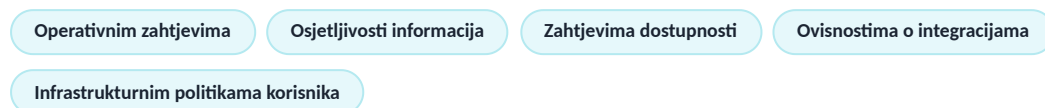
ITO rješenja mogu se dizajnirati za implementaciju unutar infrastrukture pod kontrolom korisnika i drugih odobrenih okruženja, ovisno o arhitekturi i zahtjevima konkretnog rješenja.

Sigurnosne odgovornosti stoga ovise o odabranom modelu implementacije i rada.

MODELI IMPLEMENTACIJE • OVISNO O ZAHTJEVIMA PROIZVODA I PROJEKTA



MODEL IMPLEMENTACIJE ODABIRE SE PREMA



Mrežna sigurnost

ITO rješenja dizajnirana su za rad u primjereno segmentiranim mrežnim okruženjima.

OVISNO O ARHITEKTURI IMPLEMENTACIJE, KONTROLE MOGU UKLJUČIVATI

- Razdvajanje aplikacijskih, bazodatnih, integracijskih i administrativnih komponenti
- Pravila vatrozida
- Ograničena upravljačka sučelja
- Šifriranu komunikaciju
- Kontroliranu vanjsku povezanost
- Nadzor relevantne mrežne aktivnosti



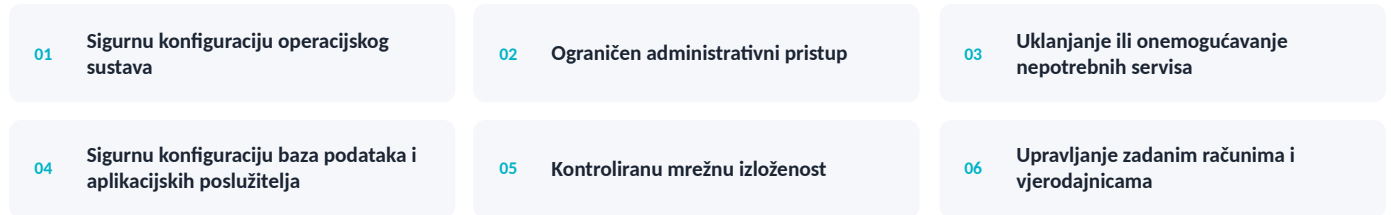
Mrežna sigurnost provodi se zajednički s korisnikom ili pružateljem infrastrukture, u skladu s dogovorenim modelom odgovornosti.

Ojačavanje, razdvajanje i otpornost

Ojačavanje sustava (hardening)

Produkcijska okruženja treba konfigurirati tako da se nepotrebni servisi, sučelja i ovlasti svedu na najmanju mjeru.

AKTIVNOSTI OJAČAVANJA MOGU UKLJUČIVATI



Zahtjevi za ojačavanje specifični za implementaciju mogu se dokumentirati kao dio implementacijskih i operativnih procedura.

Razdvajanje okruženja

Gdje je primjenjivo, razvojno, testno i produkcijsko okruženje trebaju biti logički ili fizički razdvojeni.



Dostupnost i otpornost

Zahtjevi dostupnosti razlikuju se ovisno o operativnoj kritičnosti svakog sustava. Kada to zahtijevaju arhitektura rješenja i ugovorni opseg, ITO sustavi mogu podržavati mehanizme kao što su:



Ciljeve oporavka i ciljeve dostupnosti treba definirati za svaku implementaciju u skladu sa zahtjevima korisnika i dogovorenim modelom usluge.

Sigurnost je dio inženjeringa

Sigurnost se ne može učinkovito uvesti tek na kraju razvoja softvera.

ITO stoga integrira sigurnosna razmatranja kroz cijeli životni ciklus softvera, od zahtjeva i arhitekture do razvoja, testiranja, implementacije i održavanja.

Cilj je utvrditi sigurnosne zahtjeve i potencijalne rizike što je ranije razumno moguće, kada ih je arhitekturom i dizajnom moguće učinkovitije riješiti.



Sigurnost je **životni ciklus**,
a ne kontrolna točka izdanja.

Zahtjevi, arhitektura i siguran razvoj

10.1 Zahtjevi

Sigurnost počinje razumijevanjem sustava. Tijekom analize zahtjeva relevantna razmatranja mogu uključivati:

Vrste i osjetljivost informacija

Korisničke skupine i ovlasti

Vanjska sučelja

Zahtjeve za autentifikaciju

Zahtjeve za reviziju

Regulatorne i ugovorne zahtjeve

Zahtjeve dostupnosti

Operativno okruženje

Za sustave kritične važnosti sigurnosni zahtjevi dio su ukupnih zahtjeva rješenja, a ne zasebna aktivnost nakon razvoja.

10.2 Arhitektura i dizajn

Arhitektura rješenja određuje sigurnosne granice sustava. Arhitektonske aktivnosti stoga mogu razmatrati:

Granice povjerenja

Tokove identiteta

Tokove podataka

Vanjske integracije

Povlaštene operacije

Zahtjeve za bilježenje

Mrežne granice

Scenarije kvarova

gdje je prikladno, funkcionalnostima višeg rizika posvećuje se dodatna sigurnosna pozornost tijekom dizajna.

10.3 Siguran razvoj

Od ITO razvojnih inženjera očekuje se da slijede načela sigurnog kodiranja primjerena tehnologijama i aplikacijama koje se razvijaju.

RAZVOJNE PRAKSE MOGU UKLJUČIVATI

01 Validaciju ulaznih podataka

02 Sigurnu izvedbu autentifikacije i autorizacije

03 Odgovarajuće rukovanje pogreškama

04 Zaštitu osjetljivih informacija

05 Upravljanje ovisnostima

06 Izbjegavanje poznatih nesigurnih razvojnih obrazaca

Smjernice OWASP-a mogu se koristiti kao referenca za relevantne rizike sigurnosti weba i aplikacija.

Pregled, testiranje, izdanje i održavanje

10.4 Pregled koda

Promjene koda trebaju proći odgovarajući pregled prije uvođenja u produkcijska izdanja.

MEHANIZMI PREGLEDA MOGU UKLJUČIVATI

Pregled koda od strane kolega

Tijekove rada s pull requestovima

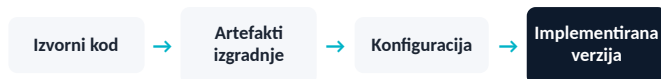
Automatske provjere

Dodatni pregled sigurnosno osjetljivih komponenti

Razina pregleda može ovisiti o riziku i složenosti promjene.

10.6 Izdanje i implementacija

Izdanja softvera trebaju slijediti kontrolirane procese koji osiguravaju odgovarajuću sljedivost između izvornog koda, artefakata izgradnje, konfiguracije i implementiranih verzija.



Implementacija u produkciju treba biti ograničena na ovlašteno osoblje ili automatizirane procese implementacije, u skladu s mjerodavnim projektnim modelom. Promjene koje utječu na sigurnosno osjetljive funkcionalnosti trebaju proći odgovarajući pregled i testiranje prije implementacije u produkciju.

10.5 Sigurnosno testiranje

Sigurnosna verifikacija može uključivati kombinaciju automatiziranih i ručnih aktivnosti, ovisno o riziku sustava i zahtjevima projekta.

One mogu uključivati:

01 Skeniranje ovisnosti i ranjivosti

02 Statičku analizu

03 Dinamičko testiranje aplikacije

04 Ručni sigurnosni pregled

05 Penetracijsko testiranje

06 Pregled konfiguracije

07 Testiranje autentifikacije i autorizacije



Ne primjenjuje se nužno svaka tehnika na svako izdanje ili proizvod. Dubina testiranja određuje se prema riziku, arhitekturi, ugovornim zahtjevima i opsegu izdanja.

10.7 Održavanje

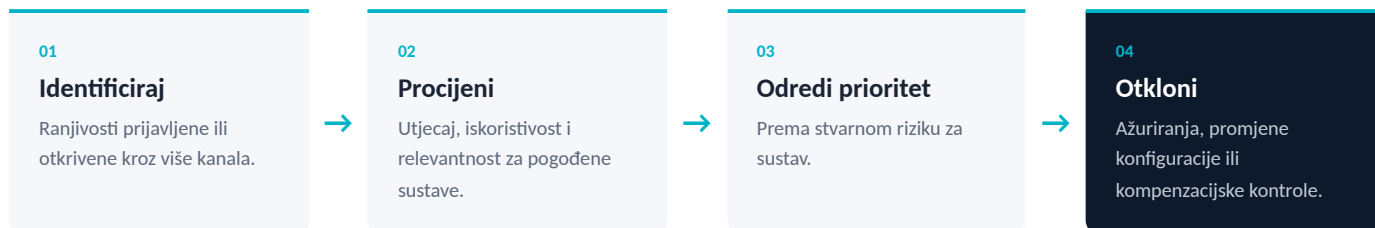
Sigurnost se nastavlja i nakon implementacije. ITO održava softver kontroliranim ažuriranjima, korektivnim izdanjima i sigurnosnim poboljšanjima u skladu s mjerodavnim aranžmanima podrške i održavanja.

Novootkrivene ranjivosti, tehnološke promjene i stečena iskustva mogu dovesti do ažuriranja aplikacija, ovisnosti, konfiguracija ili inženjerskih praksi.

Otkrivanje i upravljanje sigurnosnim slabostima

Sigurnost softvera neprestano se mijenja. Nove ranjivosti mogu se pojaviti u operacijskim sustavima, okvirima (frameworks), bibliotekama, infrastrukturnim komponentama i aplikacijskom kodu i nakon što je sustav već implementiran.

ITO stoga upravljanje ranjivostima tretira kao stalni dio održavanja softvera i upravljanja sigurnošću.



Izvori informacija o ranjivostima

Potencijalne ranjivosti mogu se otkriti kroz različite kanale, uključujući:

- Interno testiranje
- Automatizirane sigurnosne alate
- Sigurnosna upozorenja za softverske ovisnosti
- Proizvođače tehnologije
- Prijave korisnika
- Vanjske sigurnosne procjene
- Odgovorne prijave neovisnih sigurnosnih istraživača

Utvrđene ranjivosti treba procijeniti prema njihovom mogućem utjecaju, iskoristivosti i relevantnosti za pogođene sustave.

Sigurnost ovisnosti

Suvremeni softver oslanja se na biblioteke, okvire i infrastrukturne komponente trećih strana.

ITO razvojni timovi stoga trebaju pratiti sigurnosne ranjivosti koje pogađaju relevantne ovisnosti i procjenjivati ažuriranja kada je to potrebno.

Određivanje prioriteta prema riziku

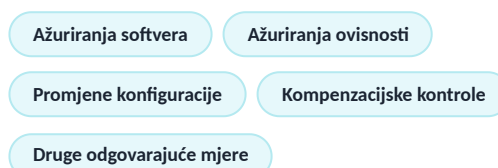
Ne predstavlja svaka objavljena ranjivost istu razinu rizika za svaki implementirani sustav. Procjena treba uzeti u obzir čimbenike kao što su:



To omogućuje određivanje prioriteta aktivnosti otklanjanja prema stvarnom riziku za sustav.

Otklanjanje

Kada se potvrdi ranjivost u komponenti koju održava ITO, otklanjanje može uključivati:



Prioritet otklanjanja treba odražavati procijenjeni sigurnosni rizik i operativni kontekst.

Sigurnost se nastavlja nakon implementacije

Implementacija ne predstavlja kraj sigurnosnog životnog ciklusa. Sustavi kritične važnosti zahtijevaju stalno održavanje, nadzor, kontrolirane promjene i jasno definirane procedure za odgovor na operativne i sigurnosne događaje.

Točan operativni model ovisi o arhitekturi implementacije i ugovornom aranžmanu. U nekim okruženjima ITO može pružati održavanje i podršku na razini aplikacije, dok infrastruktura, mrežne operacije i sigurnosni nadzor ostaju pod kontrolom institucije korisnika ili pružatelja infrastrukture kojeg je ona odredila.

Zbog toga operativne sigurnosne odgovornosti treba jasno definirati za svaku implementaciju.

PRIMJER MODELA • ITO

Razina aplikacije

Održavanje i podrška aplikacije.

PRIMJER MODELA • KORISNIK ILI ODREĐENI PRUŽATELJ

Razina infrastrukture

Infrastruktura, mrežne operacije i sigurnosni nadzor.

Sigurnosni nadzor

Ovisno o rješenju i dogovorenom operativnom modelu, nadzor može uključivati:

Dostupnost aplikacije

Pogreške sustava

Događaje autentifikacije

Neuspjehe integracija

Stanje infrastrukture

Aplikacijske zapise

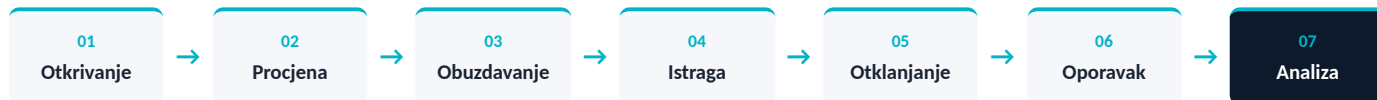
Druge sigurnosno relevantne događaje

Kada ITO ne upravlja infrastrukturom na kojoj sustav radi, odgovarajuće odgovornosti za nadzor mogu ostati na instituciji korisniku ili pružatelju usluga kojeg je ona odredila.

Upravljanje incidentima

Sigurnosni incidenti zahtijevaju koordiniran tehnički i organizacijski odgovor. ITO-ov pristup upravljanju incidentima treba podržati identifikaciju, procjenu, obuzdavanje, otklanjanje i analizu sigurnosnih incidenata koji pogađaju sustave ili usluge u području odgovornosti ITO-a.

TIPIČAN ŽIVOTNI CIKLUS INCIDENTA



Kada incident uključuje infrastrukturu pod kontrolom korisnika, institucionalne podatke ili sustave trećih strana, aktivnosti odgovora treba koordinirati s odgovornom organizacijom prema utvrđenim procedurama komunikacije i eskalacije.

Klasifikacija, komunikacija i učenje

Klasifikacija incidenata

Sigurnosne događaje treba procijeniti prema njihovom mogućem utjecaju na:



Komunikacija o incidentu

Kada potvrđeni incident pogađa okruženje korisnika u području odgovornosti ITO-a, komunikacija treba slijediti mjerodavne ugovorne, pravne i operativne zahtjeve.

ITO i institucija korisnik trebaju održavati odgovarajuće kanale eskalacije za sigurnosno relevantne događaje.

Stečena iskustva

Značajni sigurnosni incidenti trebaju pridonijeti kontinuiranom poboljšanju. Analiza nakon incidenta može otkriti prilike za poboljšanje:

Softvera

Arhitekture

Nadzora

Procedura

Dokumentacije

Edukacije

Organizacijskih kontrola

SIGURNOSNA ZRELOST

Sigurnosna zrelost nije odsutnost incidenata.

To je sposobnost da se incidenti **spriječe** gdje je moguće, učinkovito **otkriju**, na njih primjereno **odgovori** i da se sustav kontinuirano **poboljšava**.

Sigurnost seže izvan ITO-a

Sigurnost rješenja ne ovisi samo o softveru koji ITO izravno razvija, već i o tehnologijama i dobavljačima koji čine dio cjelokupnog sustava.

ITO sigurnost softverskog i tehnološkog lanca opskrbe prepoznaje kao dio svoje šire sigurnosne odgovornosti.

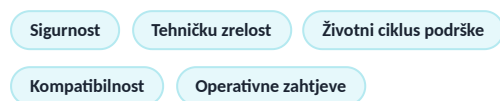


SUVREMENI TEHNOLOŠKI EKOSUSTAV

Suvremene softverske platforme ovise o tehnološkim ekosustavima koji mogu uključivati operacijske sustave, razvojne okvire, komponente otvorenog koda, baze podataka, tehnologije oblaka ili infrastrukture, hardverske uređaje i specijalizirane tehnološke partnere.

Komponente trećih strana

Softverske komponente trećih strana treba odabirati i održavati uzimajući u obzir:



Kada se utvrde ranjivosti relevantnih komponenti trećih strana, njihovu primjenjivost i mogući utjecaj treba procijeniti u sklopu aktivnosti upravljanja ranjivostima.

Softver otvorenog koda

Softver otvorenog koda može donijeti značajne inženjerske prednosti i prednosti interoperabilnosti, ali zahtijeva odgovarajuće upravljanje.

ITO treba imati uvid u sigurnosno relevantne ovisnosti trećih strana koje se koriste u njegovom softveru te procjenjivati utvrđene ranjivosti i ažuriranja prema njihovoj relevantnosti i riziku.

Tehnološki partneri i rizik dobavljača

Tehnološki partneri

ITO rješenja mogu integrirati tehnologije specijaliziranih proizvođača trećih strana kada te tehnologije pružaju mogućnosti potrebne projektu. Primjeri mogu uključivati:

Infrastrukturu identiteta	Baze podataka	Tehnologije oblaka	Skenere dokumenata	Kamere
LPR / ANPR uređaje	Biometrijske uređaje	Platnu infrastrukturu	Druge specijalizirane sustave	

Uključivanje tehnologije treće strane **ne znači automatski** da ITO kontrolira sigurnosni životni ciklus te tehnologije.

Odgovornosti stoga treba definirati prema konkretnoj integraciji i ugovornom modelu.

Rizik dobavljača

Kada dobavljači ili podizvođači mogu imati pristup osjetljivim sustavima, informacijama ili razvojnim procesima, sigurnosna razmatranja trebaju biti dio odabira dobavljača i upravljanja njima.

OVISNO O PRIRODI ODNOSA, KONTROLE MOGU UKLJUČIVATI

01 Ugovorne sigurnosne zahtjeve	02 Obveze povjerljivosti	03 Ograničenja pristupa	04 Pregled relevantnih sigurnosnih sposobnosti
---------------------------------	--------------------------	-------------------------	--

Sigurnost je podijeljena odgovornost

Sigurnost informacijskog sustava kritične važnosti ne može osigurati sam softver. Učinkovita sigurnost ovisi o koordiniranim odgovornostima pružatelja tehnologije, institucije korisnika, operatora infrastrukture, korisnika i pružatelja tehnologija trećih strana.



Tehnologija osigurava **kontrole**. Institucije osiguravaju **ovlast i upravljanje**. Sigurnost ovisi o oboje.

Tko je za što odgovoran

ITO promiče pristup podijeljene odgovornosti u kojem se odgovornosti definiraju prema arhitekturi, modelu implementacije, mjerodavnim propisima i ugovornom aranžmanu.

INSTITUCIJA KORISNIK

Ovisno o modelu implementacije i ugovora, u pravilu zadržava odgovornost za:

- Zakonitu svrhu i korištenje sustava
- Ovlaštene korisnike
- Organizacijske uloge i ovlasti
- Interne procedure
- Politike upravljanja podacima i njihova čuvanja
- Operativne odluke
- Fizičku sigurnost
- Institucionalnu infrastrukturu kojom upravlja korisnik
- Usklađenost s pravnim obvezama specifičnima za instituciju

ITO

Unutar dogovorenog opsega odgovornosti mogu uključivati:

- Siguran softverski inženjering
- Arhitekturu aplikacije
- Provedbu dogovorenih sigurnosnih kontrola
- Održavanje softvera
- Otklanjanje ranjivosti na razini aplikacije
- Tehničku dokumentaciju
- Integracijski inženjering
- Podršku za aplikaciju
- Sigurnosna poboljšanja proizvoda

PRUŽATELJ INFRASTRUKTURE

Kada se infrastrukturom upravlja odvojeno od ITO-a, može upravljati:

- Fizičkom infrastrukturom
- Virtualizacijom
- Mrežna sigurnost
- Administracijom operacijskih sustava
- Nadzorom infrastrukture
- Pohranom
- Infrastrukturom sigurnosnih kopija
- Sigurnošću podatkovnog centra

PRUŽATELJI TEHNOLOGIJA TREĆIH STRANA

Ostaju odgovorni za sigurnost i životni ciklus svojih proizvoda i usluga u skladu s mjerodavnim ugovornim aranžmanima i aranžmanima podrške.

ITO može integrirati te tehnologije, ali ne preuzima automatski odgovornost za ranjivosti ili operativne kvarove koji potječu iz samostalno upravljanih proizvoda trećih strana.

Točna raspodjela odgovornosti ovisi o konkretnom projektu i definira se prema njegovoj arhitekturi, modelu implementacije i ugovornom aranžmanu.

Dizajn za operativni kontinuitet

Za sustave kritične važnosti sigurnost uključuje sposobnost održavanja ili ponovnog uspostavljanja ključnih usluga nakon tehničkog kvara, prekida infrastrukture, kibernetičkih incidenata ili drugih neočekivanih događaja.

Zahtjeve za kontinuitet poslovanja i oporavak od katastrofe stoga treba definirati prema operativnoj kritičnosti svake implementacije.

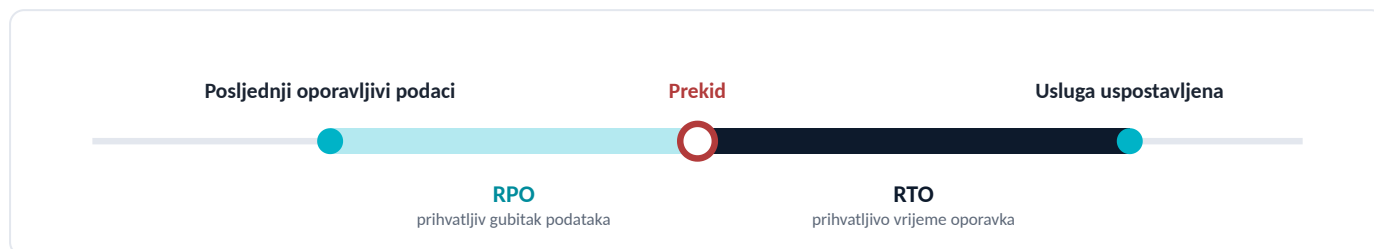
Otpornost kroz arhitekturu

Ovisno o zahtjevima projekta, mehanizmi otpornosti mogu uključivati:



Ciljevi oporavka

Ciljano vrijeme oporavka (RTO) i ciljanu točku oporavka (RPO) treba definirati u skladu sa zahtjevima korisnika i arhitekturom konkretne implementacije.



ITO ne primjenjuje jedan univerzalni cilj oporavka na sve sustave, jer se operativni zahtjevi znatno razlikuju između rješenja i institucija.

Testiranje oporavka

Mogućnosti izrade sigurnosnih kopija i oporavka od katastrofe imaju vrijednost samo ako se mogu uspješno upotrijebiti kada je potrebno. Kada aktivnosti oporavka spadaju u operativni opseg ITO-a, odgovarajuće procedure oporavka stoga treba dokumentirati i periodično provjeravati.

Sigurnost potkrijepljena priznatim standardima

ITO koristi međunarodno priznate upravljačke i inženjerske standarde kako bi osigurao strukturu, dosljednost i kontinuirano poboljšanje u svom poslovanju.

Certifikati i vanjski standardi **dopunjuju, ali ne zamjenjuju** tehničke sigurnosne kontrole. Njihova je svrha uspostaviti ponovljive organizacijske procese za upravljanje informacijskom sigurnošću, privatnošću, kvalitetom i informacijama kroz cijeli životni ciklus ITO rješenja.

CERTIFICIRANI SUSTAVI UPRAVLJANJA

ISO/IEC 27001

UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI

ITO ima sustav upravljanja informacijskom sigurnošću certificiran prema normi ISO/IEC 27001. ISMS pruža strukturirani okvir za identifikaciju rizika informacijske sigurnosti, odabir odgovarajućih kontrola, definiranje odgovornosti i kontinuirano poboljšanje praksi upravljanja sigurnošću.

ISO/IEC 27701

UPRAVLJANJE PRIVATNOŠĆU INFORMACIJA

ITO-ov okvir upravljanja privatnošću potkrijepljen je certifikatom ISO/IEC 27701. Norma proširuje upravljanje informacijskom sigurnošću kontrolama relevantnima za upravljanje privatnošću informacija i podupire sustavan pristup upravljanju odgovornostima vezanima uz privatnost.

ISO 9001

UPRAVLJANJE KVALITETOM

Upravljanje kvalitetom pruža organizacijski okvir za dosljedan inženjering, isporuku i kontinuirano poboljšanje. U ITO-u su kvaliteta i sigurnost komplementarne discipline: pouzdan softver zahtijeva kontrolirane inženjerske procese kao i odgovarajuće tehničke zaštitne mjere.

ISO 30301

SUSTAVI UPRAVLJANJA ZAPISIMA

Gdje je primjenjivo na certificirani opseg ITO-a, načela upravljanja zapisima podupiru kontrolirano stvaranje, upravljanje, čuvanje i upravljanje organizacijskim zapisima.

Ovaj se certifikat odnosi na ITO-ov organizacijski sustav upravljanja. Sam po sebi ne certificira funkcionalnosti upravljanja zapisima u ITO proizvodima.

Inženjerske i sigurnosne reference

Uz certificirane sustave upravljanja, ITO inženjerske prakse mogu se pozivati na utvrđene industrijske smjernice i standarde primjerene pojedinim tehnologijama i projektima.

One mogu uključivati relevantne smjernice:

OWASP Sigurnost aplikacije	NIST Koncepti kibernetičke sigurnosti i upravljanja rizicima	OpenAPI Dokumentirana aplikacijska sučelja	OAuth 2.0 / OpenID Connect Gdje je primjenjivo na arhitekture identiteta i API-ja	Privacy by Design Načela za sustave koji obrađuju osobne podatke
--------------------------------------	--	--	---	--

KAKO ČITATI ITO-OVE TVRDNJE O STANDARDIMA

CERTIFICIRANO Sustavi upravljanja koje neovisno revidira vanjsko certifikacijsko tijelo.	USKLAĐENO Prakse osmišljene da slijede zahtjeve okvira, bez tvrdnje o certifikaciji.	REFERENCIRANO Industrijske smjernice koje se koriste gdje su relevantne za pojedine tehnologije i projekte.
--	--	---

Ovaj whitepaper ove pojmove koristi namjerno i ne grupira ih zajedno.

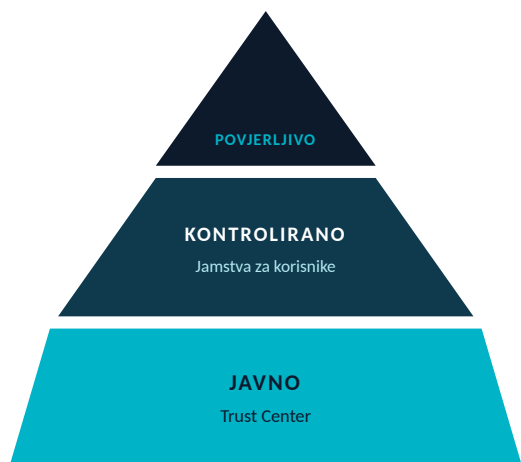
	CERTIFICIRANO	REFERENCIRANO
ŠTO ZNAČI	Neovisno revidiran sustav upravljanja	Smjernice koje se koriste gdje su relevantne
ODNOSI SE NA	ITO kao organizaciju unutar certificiranog opsega	Pojedine tehnologije i projekte
U OVOM DOKUMENTU	ISO/IEC 27001 • ISO/IEC 27701 • ISO 9001 • ISO 30301	OWASP • NIST • OpenAPI • OAuth 2.0 / OIDC • Privacy by Design

Pozivanje na industrijski okvir znači da njegove smjernice usmjeravaju ITO inženjersku praksu. To nije tvrdnja o certifikaciji prema tom okviru.

Povjerenje zahtijeva provjerljive informacije

Sigurnost zahtijeva povjerljivost, ali upravljanje sigurnošću ne bi smjelo ovisiti o tajnosti.

ITO nastoji korisnicima i partnerima pružiti dovoljno informacija da razumiju pristup sigurnosti u organizaciji, inženjerskim procesima i tehnološkim platformama, uz zaštitu informacija čije bi javno objavljivanje moglo stvoriti nepotreban sigurnosni rizik. Naš model transparentnosti stoga razlikuje javne, kontrolirane i povjerljive sigurnosne informacije.



● Povjerljivo

Detaljni sigurnosni dokazi. Dostupno samo kada je opravdano i uz odgovarajuće aranžmane o povjerljivosti.

● Kontrolirano

Jamstva za korisnike. Dostupno kvalificiranim korisnicima, partnerima ili u postupcima nabave, kada je prikladno.

● Javno

Dostupno svima putem ITO Trust Centera.

JAVNO

- Sigurnosni whitepaper
- Dokumentacija o privatnosti i upravljanju podacima
- Načela odgovorne umjetne inteligencije
- Pregled sigurnog razvoja softvera
- Informacije o certifikatima
- Politika odgovornog otkrivanja ranjivosti
- Dokumentacija arhitekture na visokoj razini

KONTROLIRANO

- Detaljni sigurnosni upitnici
- Matrice sigurnosnih kontrola
- Sigurnosna dokumentacija specifična za proizvod
- Informacije o arhitekturi implementacije
- Informacije o kontinuitetu poslovanja
- Odabrani sažeci procjena
- Dokumentacija tokova podataka

POVJERLJIVO

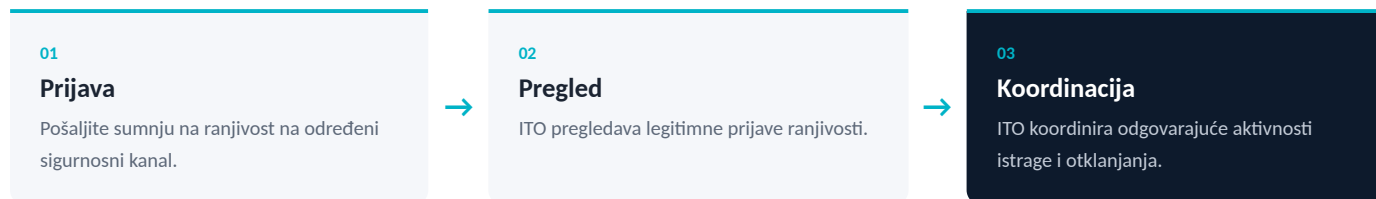
- Detaljni rezultati penetracijskih testova
- Osjetljive informacije o arhitekturi
- Interne sigurnosne procedure
- Detaljne informacije o ranjivostima
- Sigurnosne konfiguracije
- Pojednosti o odgovoru na incidente
- Druge informacije čije bi javno objavljivanje moglo bitno povećati sigurnosni rizik

Transparentnost ne zahtijeva otkrivanje osjetljivih sigurnosnih informacija. Zahtijeva pružanje pravih dokaza pravim dionicima.

Suradnja sa sigurnosnom zajednicom

ITO prepoznaje da neovisni sigurnosni istraživači mogu pridonijeti poboljšanju sigurnosti digitalnih proizvoda i usluga.

Potičemo odgovorno prijavljivanje sumnji na sigurnosne ranjivosti u ITO proizvodima, uslugama ili javno dostupnoj infrastrukturi.



Prijave trebaju sadržavati dovoljno informacija da se problem može razumjeti i, gdje je to razumno moguće, reproducirati.

KANAL ZA PRIJAVU

Pronašli ste moguću ranjivost? Javite nam.

ITO pozdravlja odgovorno prijavljivanje mogućih sigurnosnih ranjivosti u svojim proizvodima i javno dostupnim sustavima.

Sigurnosni istraživači i druge strane koje smatraju da su otkrile moguću ranjivost potiču se da kontaktiraju ITO sigurnosni tim putem određenog sigurnosnog kanala.

ODREĐENI SIGURNOSNI KANAL

security@ito.dev

TRUST CENTER

ito.dev/en/trust-center

Podrška sigurnosnoj dubinskoj analizi

Državne institucije i poslovni korisnici mogu tijekom nabave, implementacije ili periodične procjene dobavljača zatražiti dodatne sigurnosne informacije.

ITO podržava odgovarajuće procese sigurnosnih jamstava za korisnike pružanjem relevantne tehničke i organizacijske dokumentacije, ovisno o prirodi projekta i osjetljivosti traženih informacija.

OVISNO O SURADNJI, TO MOŽE UKLJUČIVATI

01 Sigurnosne upitnike	02 Dokaze o certifikatima	03 Sigurnosnu dokumentaciju proizvoda
04 Dokumentaciju arhitekture	05 Informacije o sigurnosti integracija	06 Zahtjeve za implementaciju
07 Dokumentaciju kontrole pristupa	08 Informacije o tokovima podataka	09 Informacije o kontinuitetu i oporavku
10 Informacije o upravljanju ranjivostima	11 Relevantne dokaze neovisnih procjena	

Osjetljiva dokumentacija može zahtijevati odgovarajuće aranžmane o povjerljivosti.

Sigurnosna dokumentacija specifična za proizvod

Ovaj whitepaper opisuje ITO-ov pristup sigurnosti na razini organizacije. Pojedine ITO platforme mogu imati dodatnu dokumentaciju specifičnu za proizvod koja obrađuje njihovu arhitekturu, sigurnosne kontrole, integracije, modele implementacije i operativne zahtjeve.

SIGURNOST PROIZVODA

RENATA sigurnosna dokumentacija

Sigurnosne informacije specifične za platformu RENATA, namijenjenu tijelima za provedbu zakona, dostupne su na zahtjev putem odgovarajućih kanala jamstava za korisnike.

Dostupno na zahtjev
security@ito.dev

Inženjering povjerenja

Sigurnost softvera kritične važnosti ne može ovisiti o jednoj tehnologiji, certifikatu ili kontroli.

Zahtijeva discipliniran inženjering, jasno definirane odgovornosti, sigurnu arhitekturu, kontrolirane razvojne procese, operativnu svijest i kontinuirano poboljšanje.

ITO pristupa sigurnosti kao životnom ciklusu koji se proteže od prvog zahtjeva sustava preko arhitekture, razvoja, implementacije i rada do dugoročnog održavanja.

NE SAMO

Izgraditi softver koji obavlja svoju predviđenu funkciju.

NAŠ CILJ

Razviti digitalne platforme koje institucije mogu **sigurno koristiti**, **odgovorno njima upravljati** i **razvijati tijekom vremena**.

Povjerenje se ne dodaje nakon što je softver izgrađen.

Povjerenje se ugrađuje u način na koji se softver dizajnira, razvija i koristi.



NAŠA PREDANOST

Engineering Digital Trust.



UGRAĐENA SIGURNOST • NAJMANJE OVLASTI • VIŠESLOJNA ZAŠTITA • ODGOVORNOST

Engineering Digital Trust.

Sigurnosna dokumentacija specifična za proizvod i implementaciju može dopunjavati ovaj
whitepaper. Rado ćemo podržati dubinsku analizu vašeg sigurnosnog tima za bilo koju ITO
platformu.

SIGURNOST I PRIJAVE

security@ito.dev

TRUST CENTER

ito.dev/en/trust-center

OPĆI UPITI

info@ito.ba • +387 36 830 003

TVRTKA

IT Odjel Mostar d.o.o., Mostar, Bosna i Hercegovina

DOKUMENT

ITO-TRUST-SEC-001 • Verzija 1.0 • JAVNO • Listopad 2026.