Sisukord

Directo teenuse tehniline kirjeldus

Teenuse toimimist tagavad vahendid

Serverid

Directo teenuse osutamiseks kasutatakse rakendus- ja andmebaasiservereid, mis ei teeninda mitte ühtegi muud teenusepakkujat. Kesksüsteemi teenuse (hosting, internetiühendus, turvauuendused, monitooring, riistvarahooldus jne) osutajaks on Telia Eesti AS, kelle infoturbe juhtimissüsteem on sertifitseeritud Bureau Veritas poolt ISO 27001 standardi alusel. GDPR seatud andmete säilitamise nõuded on ISO 27001 alamosa
https://www.telia.ee/images/documents/sertifikaadid/iso_iec_27001_2013_est.pdf

Andmete säilitamine

Directo kasutamise käigus tekkivaid andmeid hoitakse MS SQL andmebaasidena ning Windows Server kettapinnal. Andmed asuvad füüsiliselt Eesti Vabariigi territooriumil.

Varukoopiad

Kõikidest Directo kasutamise käigus tekkivatest andmebaasikirjetest koostatakse regulaarsed varukoopiad. Varukoopiad luuakse iga 24h tagant ajaaknas 23:00 UTC - 03:00 UTC. Varukoopiaid säilitatakse lindihoidlas, mille ainuotstarve on Directo andmete varundamine. Varukoopiad asuvad rakendusserveritega võrreldes erinevas geograafilises asukohas, kuid igal juhul Eesti Vabariigi territooriumil. Iga varukoopia sisaldab kõiki ajaloolisi andmeid ning maksimaalne võimalik andmekadu tehnilise tõrke korral piirdub viimase 24h tunni jooksul loodud või muudetud andmetega.

Töökindlus ja käideldavus

Directo kui süsteemi projekteeritud käideldavuse tase on 99.9%. Teenuse arhitektuur ei näe ette planeerimatuid töökatkestusi.

Planeeritud töökatkestuste jaoks on ette nähtud igapäevane hooldusperiood 23:00 UTC - 03:00 UTC. Hooldusperioodil toimuvate planeeritud katkestuste maksimaalne pikkus võrdub hooldusperioodi pikkusega.

Planeerimata töökatkestuse esinemise stsenaariumi korral on ette nähtud teenuse taastamine 15 minuti jooksul.

Monitooring

Directo teenuse toimimist jälgitakse automatiseeritud vahenditega 24/7. Riistvara käideldavuse

monitooringu teenust osutab Telia Eesti AS. Teenuse sisulise toimimise monitooringut teostab Directo OÜ ning selle raames jälgitakse muuhulgas, kuid mitte ainult:

- funktsionaalsete vigade ilmnemist, vigade arvu ja iseloomu
- erinevate operatsioonide täitmise aegasid ja nende vastavust seatud normidele
- teenuse toimimiseks vajalike ressursside (protsessor, mälu, ketas jne) koormatust

Monitooringu poolt tuvastatud ebaootuspärase käitumise kohta edastatakse automaatseid teavitusi administraatoritele 24/7.

Projekteeritud jõudlus

Normaaltingimustes kasutamisel loetakse süsteemi normaalseks töökiiruseks olukorda, kus lihttoimingud (dokumendi avamine, registrist vajaliku info otsimine jms) teenindatakse serveri poolt 2000ms jooksul. Selle aja hulka ei arvestata aega, mis kulub andmete edastamiseks serverist kasutaja arvutini. Mahukat infot töötlevate ja esitavate aruannete puhul ei ole ette nähtud normeeritud aruande täitmise aega, kuid aruande parameetrite valimise vaate kasutajale esitamise ajanorm on maksimaalselt 2000ms.

Ründekindlus

Süsteem on projekteeritud kõikide sisuliste rünnakute (SQL injection jms) tõrjumist silmas pidades. Seda printsiipi järgitakse kõikide arendusprotsesside juures ning pistelist ründekindluse testi viiakse läbi vähemalt kaks korda aastas.

Teenust kasutavate klientide (ettevõtete) andmed on täiendavalt isoleeritud andmebaasikihi tasandil, millega välditakse erinevate juriidiliste isikute vahelisi ristandmelekkeid.

Väljastpoolt teenusepakkuja vastu suunatud koordineeritud (DDOS) rünnakute tuvastamise ja tõrjumise teenust osutab Telia Eesti AS.

Teenuse kasutamine

Kasutamiseks vajalik tarkvara

Directo kasutamiseks on vajalik toimiv internetiühendus ja veebilehitseja. Kasutada saab kõiki levinumaid veebilehitsejaid nagu näiteks Internet Explorer, Mozilla Firefox, Google Chrome, Edge, aga kasutaja peab tagama, et installeeritud oleks valitud veebilehitseja värskeim versioon koos kõigi ametlike turvauuendustega.

Directo kasutamine ei sõltu kasutatavast operatsioonisüsteemist. Ükskõik millise Windowsi, MacOS, Linux vms operatsioonisüsteemi puhul peab kasutaja tagama, et paigaldatud on kõik värsked tootja poolt soovitatud turvauuendused.

Directo kasutamine ei eelda veebilehitsejasse lisatarkvara (Add-in ehk plugin) lisamist, kui ei plaanita kasutada ID-kaarti või riistvaraintegratsiooni (kliendiekraan, makseterminal jne), samuti siis puudub vajadus arvutisse täiendavat eraldiseisvat tarkvara installeerida.

Ühenduskanal

Directo teenust on võimalik kasutada ainult krüpteeritud HTTPS protokolli vahendusel. Ühenduse turvamiseks kasutatakse sha256RSA algoritmiga ning 4096bit RSA avaliku võtmega sertifikaati.

Autentimine

Directo kasutamine on võimalik ainult autenditud kasutajal talle määratud õiguste ulatuses. Vaikimisi toimub kasutaja tuvastamine kasutajanime ja parooli kombinatsiooniga. Soovi korral on võimalik ja soovitatav rakendada täiendavaid turvameetmeid:

1. Parooli turvalisuse tõstmine. Süsteemi seadistuses on võimalik määrata parooli keerukuse ja vahetamise sagedusele esitatavaid nõudeid, et tagada kasutajanimi/parool kombinatsiooni maksimaalne turvalisus
2. Digitaalse isikutunnistuse kasutamine. Kasutajanime/parooli asemel võib nõuda autentimist digitaalse isikutunnistuse abil. Võimalikud tuvastusvahendid on
    - Eesti Digi-ID ehk ID-kaart
    - Eesti või Läti Mobiil-ID
    - Eesti, Läti või Leedu Smart-ID
3. Kasutajate ligipääsu lubamine või piiramine IP aadressi põhiselt. Võimalik on määrata IP aadressite whitelist'e või blackliste, mis reguleerivad ligipääsu teenusele. Nimetatud piirangud võivad kasutajate lõikes erineda ja on kõikide muude autentimisvahendite suhtes ülimuslikud, st näiteks keelatud aadressilt ei õnnestu sisse logida ka ID-kaardiga.