Tietoturva

Hyvästä tietoturvasta huolehtiminen on keskeinen osa riskrate -ohjelmiston kehitystä ja palvelutuotantoa. Tietoturva kattaa mm. palvelinten ulkoisen ja sisäisen turvallisuuden, palvelussa olevien tietojen varmistamisen, sekä laitteistojen että ohjelmistojen testauksen ja seurannan, henkilöstön salassapitovelvollisuuden ja käyttäjien tunnistuksen sekä ohjelmistoon liittyvän tietoliikenteen salauksen.

Palvelinten tietoturva

riskrate -tuotantoympäristö toimii palvelimella, joihin pääsevät vain käyttöoikeudet saaneet henkilöt. Tuotantopalvelinten ylläpidosta huolehtii Amazon Web Services. Amazon Web Services on johtava konesali- ja IT-palvelutarjoaja globaalisti. Amazonin pilvessä ajetaan ohjelmistokehitys- ja testausympäristöjä, big data -analytiikkaa, mobiili-, web- ja somesovelluksia, yritysohjelmistoja, esineiden internetiä (IoT) hyödyntäviä sovelluksia sekä monia liiketoiminnalle kriittisiä työkuormia. Amazon Web Services asiakkaisiin kuuluu joukko Suomenkin nopeimmin kasvavia ja tunnetuimpia yrityksiä. Amazon Web Services tarjoaa riskraten palvelutuotannolle turvallisen ja keskeytymättömän toiminnan takaavan ympäristön.

Tietokantojen ja -järjestelmien käyttöoikeudet varmistetaan yritys- ja henkilökohtaisilla käyttöoikeusmäärittelyillä. Vain testattujen ja hyväksyttyjen ohjelmistojen käyttö on sallittua tietokantojen käsittelyssä ja ulkopuolisten hallintaohjelmistojen käyttö on estetty. Tietokantaliikenteen rajapintojen käyttö on estetty ulkopuolisesta verkosta.

Keskeytymätön toiminta, varmistukset ja valvonta

riskraten palvelinympäristössä on kiinnitetty erityistä huomiota keskeytymättömään toimintaan ja vikasietoisuuteen. Kaikki riskraten tietokannat ja tiedostot varmuuskopioidaan päivittäin erilliseen palotilaan, minkä lisäksi muuttuvia tietoja replikoidaan jatkuvasti varapalvelimelle. Palvelinkeskuksen ja palvelutuotannon tilaa seurataan, jotta mahdolliset ongelmatilanteet voidaan havaita ja korjata mahdollisimman nopeasti.

Testaus ja seuranta

Palomuurien ym. tekniikan toiminta testataan säännöllisesti. Tietoverkon ja sen palveluiden luvattomia käyttöyrityksiä seurataan aktiivisesti.

riskrate -ohjelmisto ja siihen tehtävät päivitykset testataan erillisessä testiympäristössä ennen varsinaista julkistusta. Laitteistojen ja järjestelmien lisäksi ohjelmistoon liittyviä lokitiedostoja seurataan ja analysoidaan säännöllisesti. Myös käyttäjien aiheuttamia virhetilanteita seurataan ja analysoidaan.

Useiden eri kanavien kautta hankitaan aktiivisesti tietoa tietojärjestelmiin kohdistuvista riskeistä. Hankittujen tietojen perusteella pystytään varautumaan mahdollisiin ongelmatilanteisiin sekä poistamaan niitä jo ennen niiden syntymistä.

Henkilöstön ammattitaito ja salassapitovelvollisuus

Riskraten palvelutuotantoon osallistuvaa henkilöstöä koulutetaan työtehtävien mukaisesti määritellyillä alueilla. Kaikki henkilöt, jotka ovat tekemisissä asiakkaiden luottamuksellisten tietojen kanssa, ovat allekirjoittaneet salassapitosopimuksen.

Käyttäjien tunnistus ja käyttöoikeudet

riskrate -ohjelmiston käyttäjien autentikoinnissa käytetään henkilökohtaista käyttäjätunnusta ja salasanaa.. Tiedonsiirto käyttäjän koneen ja riskraten palvelinten välillä on salattu käyttäen HTTPS-tekniikkaa.

Käyttäjän tulee välttää henkilökohtaisen käyttäjätunnuksen ja salasanan sekä vaihtuvien salasanojen luovuttamista muille. riskratesta ei oteta käyttäjään yhteyttä sähköpostitse tms. tavoilla ja tiedustella salasanaa, vaihtuvia salasanoja tai muita salaista tietoa. riskraten käyttöön liittyvistä asioista tiedotetaan pääkäyttäjien kautta sekä uutisviesteissä.