VÄIKEETTEVÕTE

PORTUGAL

3. riskilugu

Co-funded by the
Erasmus+ Programme
of the European Union

Väikeettevõte Portugalist

Ettevõtte ja tarneahela kontekst

Ligikaudu 30 töötajaga ja peaaegu 30 aastat transpordikonsultatsiooniga tegeleval ettevõttel on kolm peamist tegevusvaldkonda: liiklusuuringud, transpordivõrkude planeerimine ja avalik maanteetransport. Ettevõtte töö hõlmab muuhulgas nii raudteede planeerimist riigiasutuste jaoks kui ka kaubanduskeskuste parklate planeerimist.

Mõne planeeringu puhul on ettevõttel prognoosimudelite väljatöötamiseks juurdepääs teatavatele klientide esitatud tundlikele andmetele, näiteks klientide üksikasjalikele finantsandmetele või teatavate teede detailsetele liiklusandmetele.

Tarneahela digitaliseerimine

Ettevõttel on kaks põhisüsteemi: üks projektide finantsjuhtimiseks ja teine projektitingimuste haldamiseks. Mõlemad süsteemid on unikaalsed, spetsiaalselt ettevõtte jaoks välja töötatud ja asuvad kohalikus serveris.

Mõlemad süsteemid on siiski keerulised ja vananenud, mis seavad piiranguid kasutatavusele, arvutusvõimsusele ja skaleeritavusele ning nõuavad seetõttu igapäevaseks tööks mõningaid väliseid lahendusi, näiteks liigset Exceli-failide kasutamist.

Mõlema süsteemi arendus on pooleli. Süsteemide andmete migreerimine on samuti problemaatiline ja kallis ettevõtmine. Varem tehti süsteemi varukoopiaid iga kuu käsitsi kõvakettale, kuid hiljuti mindi üle igapäevasele varundamisele pilveteenuse kaudu.

Mõlema süsteemi piirangute tõttu toimub kogu suhtlus ülejäänud tarneahelaga muude vahendite abil, kõige sagedamini e-posti teel.

Co-funded by the Erasmus+ Programme of the European Union

Riskijuhtimine

Riskijuhtimise praktika

Delikaatsete andmete konfidentsiaalsus on praegu tagatud konfidentsiaalsuslepingute ja mitmefaktorilise autentimise abil. Mõned kõrgema taseme andmed on samuti kättesaadavad ainult projektijuhtidele ja neid ei avalikustata teistele töötajatele. Andmete kadumise vältimiseks varundab ettevõte andmeid iga päev.

Et lahendada oma sõltuvust unikaalsetest süsteemidest, on ettevõte palganud väliskonsultandid, et leida alternatiive oma praegustele IT-infrastruktuuri probleemidele. Selle tulemusena on 2021. aastaks IT-arendamiseks eraldatud suur eelarve. Loodetakse minna üle uutele süsteemidele, mis suudavad käsitleda palju andmeid, integreeruda väliste üksustega ja on tulevikus skaleeritavad, et pidada sammu ärinõuete täitmisega. Lõpetatud projektid jäävad vanasse süsteemi ja varukoopiatesse; ainult aktiivsed projektid liiguvad uutesse süsteemidesse, et vähendada andmete migratsioonikulusid.

Riskid

Kuna tuginetakse ettevõtte serverites asuvatele ainulaadsetele süsteemidele, võib üks süsteemi rike ohustada kogu ettevõtet pikaks ajaks. Süsteemides esineb tõrkeid ja ettevõttes on saadaval ainult üks tehnik.

Erilist tähelepanu tuleb pöörata detailsete ja tundlike andmete kasutamisele. Seega muutub küberturvalisus hädavajalikuks. Kuid kui on ainult üks IT-töötaja ja osa teavet jagatakse e-posti teel, võib turvalisus olla tõsiselt ohustatud.

Kahe süsteemi rike tähendaks ettevõtte töö seiskumist kogu rikke kestuse ajal. Kui vanad serverid aeguvad, oleks kahju märkimisväärne. Selle tulemusel võib ettevõtte äritegevus mitmeks nädalaks seiskuda, kuna kahjude kõrvaldamiseks kulub aega või puudub juurdepääs tähtsatele andmetele.

Co-funded by the Erasmus+ Programme of the European Union

Tõsine probleem oleks ka tundlike andmete leke. See kahjustaks ettevõtte mainet ja oleks vastuolus allkirjastatud konfidentsiaalsuslepingutega, mille tulemuseks võivad olla parandustööd lepingu rikkumise eest või ettevõtte töö edaspidine keelustamine paljudes tundlike andmetega seotud valdkondades.

Küberriskid

Delikaatsete andmetega tegelemine on risk, seega peaks kokkupuude internetiga ja töötajatega olema võimalikult piiratud. Delikaatsete andmete hoidmine ainult intranetis, millele on juurdepääs vaid vähestel inimestel, aitab vähendada andmelekke võimalust.

COVID-19-ga seotud riskid

Alates COVID19-epideemiast on enamik töötajaid töötanud kodus, kasutades oma privaatvõrku, et pääseda VPN-teenuste kaudu ligi tööga seotud e-kirjadele ja süsteemidele. Seega suureneb pahavara süsteemi sattumise oht ja vaja läheb täiendavaid küberturvalisuse meetmeid, kuna rohkem juurdepääsupunkte süsteemidele tähendab ka potentsiaalselt rohkem turvaauke.

Riskijuhtimise eelised:

Mitmefaktorilise autentimise ja konfidentsiaalsuslepingute abil vähendab ettevõte tundliku teabe kadumise ja lekkimise ohtu.
Investeerimine uutesse IT-lahendustesse tagab, et ettevõte saab töödelda rohkem teavet ja toiminguid ilma süsteemi seisakuteta, tagades samal ajal suurema skaleeritavuse.

Co-funded by the Erasmus+ Programme of the European Union