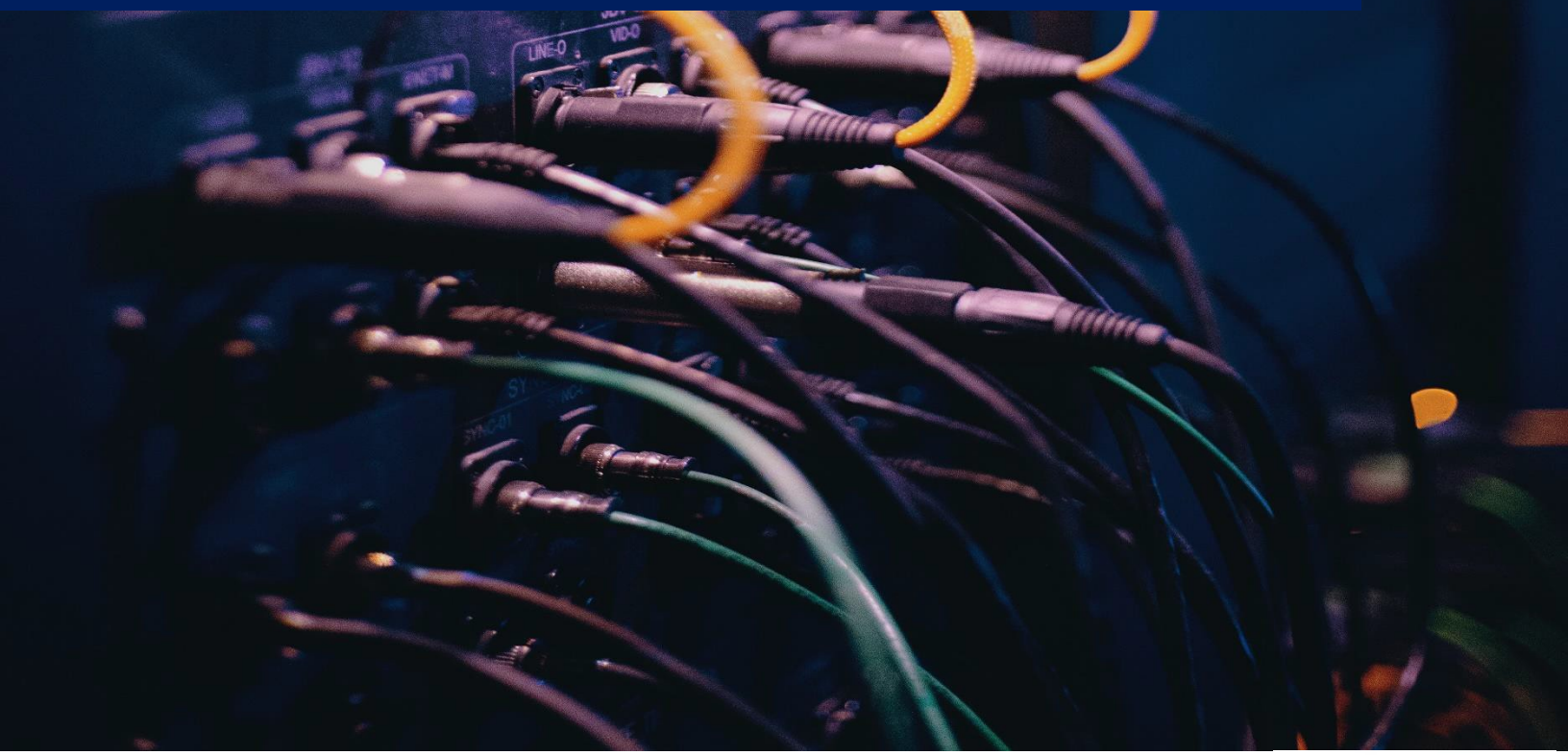
VÄIKEETTEVÕTE

AUSTRIA

5. riskilugu



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

Väikeettevõte Austriast

Ettevõtte ja tarneahela kontekst

Ettevõte on 2006. aastal asutatud keskmise suurusega ettevõte, millel on umbes 30 töötajat ja mis on spetsialiseerunud turvateenustele ja turvakonsultatsioonile. Ettevõte teostab turvalisuse või IT-penetratsiooni teste. Ettevõtteid testitakse kaitsemeetmete osas ja püütakse saada IT-süsteemi üle kontrolli ilma eelneva teadmiseta. See on üks osa portfellist, teine on põhjalik konsultatsioonipakett, mis hõlmab enamat kui rünnak. Seejärel koostatakse tegevuskava, et klient oleks tulevikuks paremini ette valmistatud ja suudaks end paremini kaitsta.

Tarneahela digitaliseerimine

Ettevõttel on kõrge digitaliseerituse tase. Kogu ärimudel põhineb kaasaegsetel tehnoloogiatel, mis on tekkinud digitaliseerimise käigus.

Riskijuhtimine

Kõik partnerid vastutavad riskijuhtimise eest.

Riskijuhtimise praktika: Töötajatel on palju lugemis- ja redigeerimisõigusi, sest neil on kõrge teadlikkus turvalisusest. Ülesande- ja kliendivaldkonnad on väga rangelt eraldatud, et iga töötaja saaks juurdepääsu dokumentidele, kus toodet parajasti arendatakse. Mis tahes metoodika, tooteinfo või tehnoloogia on juurdepääsetav. Kuid klienditeabele pääsevad juurde vaid vähesed kliendiga seotud töötajad. Kohaldatakse teadmisvajaduse põhimõtet ja juurdepääs kõigele, mis puudutab kliendiandmeid, on äärmiselt piiratud.

Riskid: Praegu puutub ettevõte peamiselt kokku tegevus- ja COVID-19 riskidega.

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

- Tegevusrisk: Pärast seda, kui klient alustab koostööd, tehakse esialgne hinnang olukorrale, töötatakse välja parendusvõimalused ja parandatakse neid dialoogis kliendiga. Riskiks on see, et töötajad käitlevad kliendi andmeid kas hooletult või ettevaatamatult ning andmed lähevad kaduma või need müüakse maha. Kui see juhtub, toob see kaasa kohtuprotsessi ja ettevõtet ähvardab tõsine mainekahju.
- Finantsrisk: Konkreetsetest riskidest ei ole teatatud.
- Tururiskid: Konkreetsetest riskidest ei ole teatatud.
- Küberriskid: Konkreetsetest riskidest ei ole teatatud.
- COVID-19-ga seotud riskid: Eelkõige pandeemia ajal suureneb probleem, et turvakontseptsioonidele tuleb eraldada piisavalt ressursse, nii rahalisi kui ka inimressursse, ning et juhtkond ja ka IT-juhid peavad selleks aega võtma. Suurim väljakutse on ressursid ja teadlikkus.

Riskijuhtimise eelised: Teadmisvajaduse põhimõte annab kontrolli ja standardiseerib teabevahetuse. Kliendiandmed edastatakse ainult valitud isikute kaudu. Kõigi asjaosaliste spetsialistidega konsulteeritakse uuesti, enne kui midagi välja saadetakse. Riskijuhtimise puhul kasutatakse andmete ja klientide andmete kaitsmiseks mitmeid vahendeid. Klassifitseerimist, mitut krüpteerimislahendust, mitut mitmefaktorilist autentimist, erinevaid e-posti kaitsesüsteeme, e-posti sertifikaate, varundussüsteeme ning varundussüsteemide ja andmete mitut asukohta.

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