RIIGI INFOSÜSTEEMI AMET

OHUHINNANG 7. märts 2022

Kokkuvõte
Eesti avaliku sektori asutustel puudub tihti ülevaade välistest arenduspartneritest, kes on kaasatud IT-hangetesse peatöövõtja juures allhankijana. Juhul, kui allhankija töötaja on pärit või asub Eesti kontekstis ebasõbralikus või riskiriigis (hetkel käsitleme nendena Vene Föderatsiooni ja Valgevenet), tuleb käsitleda tema ligipääsu või teadmisi Eesti avaliku sektori arendustele kui kõrget riski Eesti vastava avaliku sektori asutuse digitaristule. Soovitame avaliku sektori asutustel oma hankepartneritega üle kontrollida, milline on nende Vene Föderatsioonis ja Valgevenes töötavate allhankijate risk ning kuni ohuhinnangu muutmiseni edaspidi hangetes välistada riskiriikides asuvate alltöövõtjate kasutamist.

Riski kirjeldus
Eesti infoturbestandard E-ITS loetleb hulga võimalikke ohtusid, millega tuleks arvestada riskiriikidest pärit alltöövõtjate kontekstis. Nendeks on muu hulgas spionaaž, pealtkuulamine, aga ka sundus, väljapressimine ja korruptsioon (nimekiri alusohtudest on kättesaadav E-ITS portaalis). Nimetatud ohud võivad väljenduda igal pool, kuid Vene Föderatsiooni ja Valgevene puhul võib Ukraina sõja kontekstis olla nende riikide eriteenistustel eriline motivatsioon neid töötajaid mõjutada.

Arvestada tuleb asjaoluga, et riskiriigis viibija on kohalike võimude pidevas huvisfääris, mille eesmärgiks on saada juurdepääs temale kättesaadavale huvitavale informatsioonile, seda vajadusel ka isikule ettepaneku tegemisega koostööle asumiseks või kompromiteerimisega. Vene Föderatsiooni ja Valgevene pinnal asuva alltöövõtja puhul ei saa eeldada, et töötajaga sõlmitud konfidentsiaalsusleping oleks piisav meede nimetatud riskide vähendamiseks. Tuleb eeldada, et riskiriikide eriteenistused on teadlikud, kes nende kodanikest pääseb ligi Eesti riigi digitaristule ning neid võidakse jälgida, halvemal juhul tehakse koostööd digiteenuste baastaristu, arhitektuuri ja arenduse kohta andmete kogumisel. Kokkupuude meie digitaristuga võib olla ohtlik ka riskiriigis viibivale arendajale endale.

Potentsiaalne mõju
Riskiriikide eriteenistuste poolt kompromiteeritud alltöövõtja tõttu võib kasvada edukate rünnakute kasv Eesti digiteenuste ja e-riigi baastaristu vastu, kuna ründaja on teadlik asutuste võrkudest ja keskkondadest, ühendustest ja tehnoloogiatest koos nende võimalike nõrkustega. Lisaks on ohus nii klientasutuse partnerite enda süsteemid ja tekib võimalus nende kaudu rünnata teisi.

Vene eriteenistuste küberoperatsioonid kasutavad tihti ära sarnaseid tarneahelarünnakuid. Ka 2022. aastal ning Venemaa-Ukraina konflikti ajal on näha olnud, kuidas IT-teenusepakkuja kaudu on saadud ligipääs Ukraina avaliku sektori koduleheküljedele ja digitaristule ning seejärel hävitatud või varastatud andmeid.

Soovitused
Riski vähendamist ei suuda hetkel tagada ükski organisatsioon ei konfidentsiaalsuslepingute ega ka tehniliste meetmete rakendamisega. Seetõttu soovitame hankepartnerite puhul leida võimalusi vältida sellist olukorda juba algusest peale.

Soovitame hangete koostamise käigus nõuda oma hankepartneritelt ja nende allhankijatelt kindlatele kriteeriumitele vastavaid teenuse andjate taustakontrolle ja keelduda kriteeriumitele mittevastavate allhankijatega teenuse kasutamisest. Üheks kriteeriumiks peab olema riskiriigi kodanike allhangetes kasutamise vältimine.