TOK018

Turvatoimet alusöljyvahingon rantatorjunnassa

Turvariskien arviointi:
- torjuntatyöhön ja operaatioon osallistuvien henkilöstöturvaan liittyvät uhat
- kiinteistö- ja toimitilaturvaan liittyvät uhat, tilojen luokittelu ja kulunvalvonta
- Tietoturvaan liittyvät uhat: Mitä tietojen virheellisyydestä, tietojärjestelmien toimimattomuudesta, virheistä tai tietovuodoista voi seurata torjuntatyölle?
- ympäristöturvaan liittyvät uhat, vastuukysymykset, työntekijöiden ja alihankkijoiden ohjeistus
- rikosturvaan (varkaudet, vandalismi) liittyvät riskit

Turvariskien hallinta:
- turvallisuus- ja riskienhallintapäällikön nimeäminen
- henkilöstön koulutus ja perehdyttäminen torjuntaoperaation turva-asioihin
- tiedonkulun varmistaminen, työmaapiirrokset ja turvamerkinnät (poistumistiet, sammutusvälineet)
- ennakkotoimenpiteiden suhteuttaminen mahdolliseen uhkaan

Ennaltaehkäiseviä toimenpiteitä ja keinoja:

Henkilöstöturva
- avainhenkilöiden tunnistaminen, työtehtävässä tarvittavan ammattitaidon määrittäminen ja sijaisjärjestelyt
- henkilöstön liikkumisen ja toiminnan rajoittaminen, esim. kulunvalvonta organisaation tiloissa sekä erilaiset käyttäjäroolit ja niiden mukainen tietojen saatavuus tietojärjestelmissä
- tietojen päivittäminen käyttöoikeuksista ja valtuuksista sekä henkilöstön hallussa olevasta omaisuudesta

Kiinteistö- ja toimitilaturva
- kulkuluvat ja -kortit, avainten hallinta
- vartiointi, kameravalvonta, murtohälyttimet
- syttyviä materiaaleja ei säilytetä rakennusten seinustoilla (myös logistiset pisteet etäällä rakennuksista)
- tarpeettoman palokuormituksen, kuten puutavaran, varastoimista vältetään varastoissa ja niiden lähellä

Tietoturva
- nimettävä tietoturvallisuuden vastuuhenkilöt ja rajattava järjestelmävalvojan oikeudet
- huolehdittava tietoaineiston turvaamisesta ja varmuuskopioinnista
- mietittävä tietoaineiston turvallinen säilytys ja hävittäminen, sovittava missä perustiedot pidetään: SYKEn verkossa, pelastuslaitoksella vai muualla?
- henkilötietojen käsittelyssä noudatettava henkilötietolakia
- järjestettävä turvallinen internetin käyttö johtokeskuksissa ja ajantasainen virustentorjunta sekä käytettävä teknisiä ja ohjelmallisia palomuureja
- huolehdittava sähköpostin turvallisuudesta esimerkiksi yhteisissä johtokeskuksissa
- varmistettava puhelinturvallisuus ja ehkäistävä tietovuotoja ottaen huomioon myös muiden kuin viranomaistoimijoiden ohjeistus

Rikosturva
- Varkauksien ehkäisemiseksi on nimettävä vastuuhenkilö, esimerkiksi työmaajohtaja.
- Koko henkilöstöä ohjeistetaan huolellisuuteen laitteiden käsittelyssä ja ovien lukitsemisessa sekä tiedottamaan esimiestään epätavallisesti käyttäytyvistä asiattomista henkilöistä.
- On järjestettävä riittävä valaistus ja tarvittaessa hälytysjärjestelmät, mm. kameravalvonta tai vartiointi.
- Kulkukortit ja avaintenhallinta: on kirjattava ylös, kenellä avaimet on ja mitkä avaimet.
- Suunnittele toiminnallinen turvallisuus: kaikki miehittämättömät tilat pidetään lukittuina ja vain käytössä olevat tilat, varastot ja veneet lukitsematta.
- Älä jätä arvokasta tavaraa ”ei vankkoihin” rakennuksiin, esimerkiksi työmaakoppeihin.

Kannattaa laatia kirjalliset ohjeet, jotka koskevat
- kulkulupia, avainten hallintaa ja ovien lukitusta
- tietoturvaohjeita
- raportointia ja kirjanpitoa
- toimintaa erilaisissa poikkeus- tai kriisitilanteissa.