Liite 2.5 Vesihuoltolaitoksen kyberturvallisuuden tason testauksen työpöytäharjoituksen toteutussuunnitelmalomake

|  |  |
| --- | --- |
|  | 1.4.2015 |
|  |  |
| Harjoituksen nimi: | Vesijärven vesihuoltolaitoksen harjoitus 2015 |
| Ajankohta: | 1.6.2015 |
| Aihe:  | Laitoksen kyberturvallisuuden tason testaus |
| Tavoitteet: | * Selvitetään laitoksen kyberuhkiin varautumisen ja suojautumisen taso.
* Tuodaan esiin kehittämistarpeita kyberuhkiin varautumisessa ja suojautumisessa.
* Lisätään henkilöstön tietämystä kyberuhista ja niihin suojautumisesta.
 |
| Fasilitoijat: | Harjoituksen vetää ja fasilitoi esim. konsultti tai vesihuoltolaitoksen johtaja.  |
| Tarkkailijat ja arvioijat: | Tarkkailijoiksi kutsutaan esim. naapurilaitoksen henkilöstöä tai asiantuntijakonsultti. |
| Osallistujat (lkm): | Laitoksesta ja harjoituksen rajauksesta riippuen seuraavia:* vesihuoltolaitoksen johtaja
* automaatiosta vastaava
* toimialapäälliköt
* automaatiota käyttävät
* tietojärjestelmistä vastaava
 |
| Harjoitusta edeltävät valmistelut ja tarkastukset: | * Harjoituksen suunnitteluryhmän edustaja kutsuu harjoituksen osallistujat ja pyytää heitä ottamaan harjoitukseen mukaan varautumissuunnitelmat, sekä automaatio- ja tietojärjestelmien kuvaukset.
* Harjoituksen suunnitteluryhmä voi aiheeseen orientoitumiseksi laatia laitokseen perustuvan esimerkin kuvauksen kyberhyökkäyksen aiheuttamasta häiriöstä.
* Selvitetään yleisellä tasolla kyberhyökkäyksen mahdollistavia heikkouksia ja vaaroja sekä niiden mahdollisia vaikutuksia laitokselle ja laaditaan aiheesta luento harjoitukseen (voidaan tilata konsultilta).
 |
| Harjoituksen vaiheittainen eteneminen ja käytettävä aika: |  |
| 1.  | Harjoituksen avaus ja tausta, 15 min. |
| 2. | Luento kyberuhista ja niiden mahdollisista seurauksista vesihuoltolaitoksella, 1h. |
| 3. | Mahdollisen harjoitusskenaarion esittely aiheeseen orientoitumiseksi, tehtävänanto ja ohjeet työskentelyyn, 15 min |
| 3. | Ryhmätyö, jossa pohditaan seuraavia asioita laitoksen toiminnassa, osallistujat, fasilitoija ohjaa tarvittaessa keskustelua ja antaa lisäsyötteitä, ryhmässä on kirjuri, joka kirjaa havaintoja, 2 h sisältäen lounastauon * Miten vesihuoltolaitos on suojautunut automaatio- ja ohjausjärjestelmiä uhkaavien haittaohjelmien varalle? Pohdittavia asioita esim.: kohteiden kulunvalvonta, vartiointi, suojaus ja avaintenhallinta; ulkopuoliset toimijat kohteissa; tietojärjestelmien ja automaatiojärjestelmän erilaiset yhteydet muihin järjestelmiin ja internetiin; automaation taso; mahdollisuus käsin ohjaukseen; kaukovalvontatietojen kattavuus ja varmistus; päivystyskäytännöt; henkilöstön osaaminen ja taustat (turvallisuusselvitykset), myös tilapäiset; atk-järjestelmien suojaus: salasanat, virustorjunta ja varmuuskopiot; tietojärjestelmien ja automaation sähkönsaannin varmistus ja käynnistyminen sähkökatkon jälkeen;
* Miten tunnistetaan tilanne, jossa haittaohjelma on jo päässyt järjestelmään, miten vaikutukset minimoidaan ja tilanne korjataan tietojärjestelmän ja automaation osalta?
 |
| 4. | Yhteenveto, palaute ja loppukeskustelu, osallistujat, 1,5 h* Tehtyjen havaintojen purku
* Tarkkailijan kommentit harjoitukseen
* Havaitut puutteet ja muut johtopäätökset
* Muu palaute harjoituksesta
* Harjoituksen jälkitoimet
 |
| Harjoituksen jälkitoimet: | * Havaittujen puuteiden edellyttämät toimenpiteet.
* Havaittujen koulutustarpeiden täyttäminen.
* Mahdollinen jatkoharjoitus esim. henkilöstön kouluttamiseksi tai järjestelmien suojauksen vahvuuden testaamiseksi toiminnallisena harjoituksena esim. seuraavana vuonna.
 |
| Liitteet: |  |