cyVETsecurity

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

LAITTEEN TURVALLINEN KÄYTTÖ EPÄTURVALLISESSA DIGITAALISESSA MAAILMASSA

Dokumentti opettajille

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Haasteen kesto

24 tuntia / 3 päivää

Tilanteen kuvaus

Olet saanut uuden digitaalisen laitteen lahjaksi (opettajan pitäisi tarkentaa mikä laite / laitteet, jotka otetaan käyttöön), Vastuullisena digitaalisena käyttäjänä haluat yrittää varmistaa, että laita ja tiedot ovat suojattuja.
Suunnittelet käyttäväsi laitetta yleisesti, esimerkiksi käyttämällä sähköpostia, sosiaalista mediaa ja verkkopankkia ja selailemalla verkkosivuja,

Haasteenasi on näyttää, että ymmärrät ja olet tietoinen tietoturva-aiheista, jotka ovat luontaisia uusissa digitaalisissa laitteissa.

Oppimistavoitteet

U1LO1. Oppija osaa tunnistaa fyysisiä ja virtuaalisia riskejä, jotka liittyvät teknologiaan
U1LO2. Oppija osaa soveltaa riskien ehkäisyn strategioita ja pitää tietonsa ajan tasalla
U1LO3. Oppija osaa ladata ja päivittää virus/haittaohjelmatorjuntaohjelmiston
U1LO4. Oppija osaa suojata itsensä väärinkäytöksiltä käyttämällä turvallisia salasanoja
U1LO5. Oppija osaa suojata erilaisia haavoittuvia laitteita digitaalisilta uhilta (haittaohjelmat, kalastelu jne.)
U1LO6. Oppija osaa tunnistaa arkaluontoisen / arvokkaan informaation ja hyökkäykset erityyppisessä datassa

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Minimivaatimukset haasteen tekemiseen

Edeltävä tieto	Laitteet/ software	Koulutusresurssit
Verkkoyhtedellä olevan laitteen, kuten tietokone, kannettava tietokone, tabletti tai älypuhelin, käyttökokemus.	Verkkoyhteydellä oleva laite, kuten: Tietokone Kannettava tietokone Älypuhelin Tabletti	• https://en.wikipedia.org/wiki/Computer_security • https://en.wikipedia.org/wiki/Digital_security • https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more • https://passwordsgenerator.net • https://howsecureismypassword.net/ • https://www.roboform.com/how-secure-is-my-password • https://lastpass.com/howsecure.php Tästä osasta on paljon resursseja saatavilla. Opettajien tulisi käyttää kaikkia saatavilla olevia resursseja. Nämä ovat resurssit, jotka on annettu opiskelijoille haasteen ratkaisemiseen.

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Haasteen aikataulu

Alla **ehdotus** kuvitteellisesta aikataulusta haasteelle:

- 2 tuntia haasteen parametrien selvittämiseen (mahdollisesti sisältäen sen selvittäminen kuka tekee minkäkin tehtävän / tehtävät)
- 10 tuntia informaation etsimiseen
- 2 tuntia informaation valintaan
- 2 tuntia vaihtoehtojen tuottamiseen
- 2 tuntia ehdotuksen esittämiseen / löydösten kokoamiseen ja niistä keskusteluun (opiskelijaryhmässä)
- 1 tunti löydösten esittämisen selvittämiseen (jos ei vaatimuksia opettajalta)
- 2 tuntia löydösten valmisteluun tiettyyn formaattiin, esimerkiksi PowerPoint-esitys
- 2 tuntia löydösten esittämiseen / keskusteluun
- 1 tunti itsearvioinnin tekemiseen: miten haaste tehtiin ja miten voi parantaa tulevaa toimintaa

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Tulosten esittäminen

Löydökset voidaan esittää missä tahansa ryhmän päättämässä mediassa. Löydökset pitää olla sellaisessa muodossa, että ne voidaan säilyttää haasteen jälkeen. Löydösten esittely voi sisältää nämä formaatit, mutta ei rajoitettuna näihin:

- Video
- Softwarea hyödyntävä esittely
- Suullinen / verbaalinen (tämä pitäisi nauhoittaa)
- Kirjallinen raportti
- Blogi / vlogi/wiki
- Mikä tahansa muu sopiva media

Huom: Opettajan pitäisi päättää soveltuva formaatti tulosten esittämiseen.

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Arviointikriteerit

Seuraavat *ohjeet* ovat vain **ehdotuksia** ja ne ovat opettajan tukemiseksi.

Julkinen esittäminen (20%)

Ehdotettu arviointitaulukko ***Liite A*** löytyy tämän dokumentin lopusta, josta löytyy kriteerit, joita voidaan käyttää apuna julkisen esittämisen taitojen arvioimiseksi.

Tiimityön suoritus (20%)

Ehdotettu arviointitaulukko ***Liitteessä B*** löytyy tämän dokumentin lopusta, joka voi auttaa opettajaa tiimityöskentelytaitojen arvioinnissa,

Löydökset haasteesta (60%). Mahdollisesti 10% per kohta.

1. Tiimisi ryhmittelee monipuolisia riskejä 3 fyysisiin ja 3 virtuaalisiin riskeihin.

Mahdollisia opiskelijavastauksia:

Fyysisiä riskejä	**Virtuaalisia / Software riskejä**
Laitteen jättäminen valvomatta / laite varastettu	Laitteella ei ole anti-virusohjelmaa
Vesivahinko laitteessa	Uusimman softwaren päivittämättä jättäminen (korjaus)
Salasanasi antaminen jollekin	Heikot turvallisuustiedot laitteessa (salasana, pin jne.)

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

2. Tiimisi kuvaa strategian, jolla ehkäistään riskejä.

Asiat, jotka ***pitäisi*** kuulua strategiaan (laitteen käyttäjän):

- Laitteen sisäänpääsyn rajoittaminen vaatimalla käyttäjän tunnistautumista (tämän tulisi sisältää korostetutusti pin / biometrinen tunniste (esim. sormenjälki) / vahva salasana, Kaksivaiheinen tunnistautuminen (2FA) pitäisi olla myös **mainittuna**, koska tällä hetkellä se on suuntauksena käyttäjän tunnistautumisessa.)
- Päivitä laitteesi käyttöjärjestelmä uusimmilla turvallisuuskorjauksilla.
- Varmuuskopioi säännöllisesti datasi.
- Käytä kryptattua / turvallisia verkkosivuja aina kun mahdollista
- Ota pois käytöstä käyttämättömät palvelut, kuten wifi ja Bluetooth.
- Ole valveutunut (mahdollisuuksien mukaan), älä lankea kalasteluun tms.
- Pidä ajantasainen haittaohjelmaohjelmisto asennettuna.

3. Tiimisi asentaa / päivittää virus/haittaohjelmaohjelmiston annetulle laitteelle.

Tämä voi olla uuden haittaohjelmaohjelmisto (AM) asentaminen tai sen varmistaminen, että nykyinen haittaohjelmaohjelmisto käyttää uusinta versiota. NIST.org -sivulta löytyy lista ohjeista käytössä olevista haittaohjelmaohjelmistoista: https://www.nist.org/news.php?extend.45.11

Se sisältää myös ilmaisen palvelun, jossa käyttäjä voi ladata minkä tahansa tiedoston etäskannattavaksi: https://www.virustotal.com/gui/home/upload. Tämä voi olla hyödyllinen, jos käyttäjä ei voi tehdä skannausta paikallisesti laitteellaan.

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

4. Tiimisi luo ja testaa turvallisen salasanan.

- Opiskelija ***voi*** käyttää näitä linkkejä, jotka ovat resurssiosiossa.
- Salasanan luominen; https://passwordsgenerator.net
- Luodun salasanan testaaminen:
  https://howsecureismypassword.net/
  https://www.roboform.com/how-secure-is-my-password
  https://lastpass.com/howsecure.php

5. Tiimisi tunnistaa potentiaalisia, haavoittuvia laitteita ja mahdollisia mekanismeja niiden suojeluun.

Tämän pitäisi sisältää vähintään 3 potentiaalista haavoittuvuutta ja mahdollisia suojausmekanismeja, kuten:

Potentiaalisia haavoittuvuuksia	**Lieventäminen**
Uusi laite saapuu ilman tunnistautumista.	Ota käyttöön tunnistautuminen laitteessa.
Palvelut, kuten wifi ja Bluetooth ovat automaattisesti käytössä ja ne voivat vaarantua.	Sulje kaikki käyttämättömät tai tarpeettomat palvelut.
Haittaohjelman lataaminen, johon voi olla sulautunut uusia sovelluksia.	Lataa vain suositelluista verkkosivuista / paikoista. Varmista, että haittaohjelmaohjelmisto on asennettu ja ajan tasalla.

6. Tiimisi tunnistaa arkaluontoisen datan ja mahdolliset hyökkäykset datan luonteesta riippuen.

Alla joitakin ***esimerkkejä***:

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Alusta / huolenaihe	Datan tyyppi	Hyökkäyksen vektori
Sosiaaliset verkostot	Henkilökohtaiset tiedot (PII)	Sosiaalinen tekniikka, kalastelu jne.
Verkkopankki	Taloudellinen ja henkilökohtaiset tiedot (PII)	Sosiaalinen tekniikka, kalastelu jne.
Vanhan viestin heittäminen roskiin	Taloudellinen ja henkilökohtaiset tiedot (PII)	Roskisdyykkaus
Sähköposti	Kuvat / valokuvat	Steganografia (tiedon kätkeminen kuvien sisään)

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

cyVETsecurity

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

Liite A

Esityksen arviointi (Tiimi tai henkilökohtainen)

Kriteeri	Erinomainen	Erittäin hyvä	Hyvä	Kohtalainen	Ei tehty	Kommentit / ehdotukset:
Suullinen johdanto: Puhujan esittely, yleisön huomion vangitseminen	4	3	2	1	0	
Puheen sisältö: Helppo seurata ja ymmärtää, informaatio vaikuttaa täsmälliseltä ja valmiilta	4	3	2	1	0	
Yhteenveto: Lyhyt, selkeä ja tarjoaa aiheesta koonnin	4	3	2	1	0	
Suoritus: Puhuja käytti hyvää äänen vaihtelua, kunnollista ääntämistä, käytti ilmaisuja asioiden havainnollistamiseen, vaikutti keskustelevalta ja luonnolliselta, piti katsekontaktin yleisöön ja ääni oli tarpeeksi kuuluva ja selkeä kuulemiseen, tukeutui vain vähän muistilappuihin	4	3	2	1	0	
Osallistujan tiedot: Osallistuja osasi vastata yleisöstä nouseviin kysymyksiin, kysymyksen kertaamisen jälkeen	4	3	2	1	0	
Yleisön huomio: Piti yleisön huomion koko esityksen ajan.	4	3	2	1	0	
Lähteet: Lähteet olivat listattuna puheen lopussa	1	0	0	0	0	

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

cyVETsecurity

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

Liite B

Tavoitteet						
Tavoitteet ovat epäselvät tai huonosti ymmärrettyjä, joka johtaa vähäiseen sitoutumiseen niihin.	1	2	3	4	5	Tavoitteet ovat selkeät, ymmärretyt ja tiimin jäsenet ovat niihin täysin sitoutuneita
Avoimuus						
Jäsenet ovat varovaisia keskustelussa.	1	2	3	4	5	Jäsenet ilmaisevat ajatuksiaan, tunteitaan ja ideoitaan vapaasti.
Molemmin puolinen luottamus						
Jäsenet ovat epäluuloisia toistensa motiiveista.	1	2	3	4	5	Jäsenet luottavat toisiinsa ja eivät pelkää pilkkaa tai kostoa.
Asenteet erilaisuutta kohtaan						

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Jäsenet siloittavat ja tukahduttavat erilaisuuden tai välttelevät konfliktia.	1	2	3	4	5	Jäsenet tuntevat olevansa vapaita ilmaisemaan erilaisuuden ja työstämään niitä.
Tuki						
Jäsenet ovat vastahakoisia kysymään tai antamaan apua.	1	2	3	4	5	Jäsenet tuntevat olonsa mukavaksi apua antamalla ja saamalla.
Osallistuminen						
Keskustelua dominoi yleensä muutama jäsen.	1	2	3	4	5	Kaikki jäsenet osallistuvat keskusteluun.
Päätöksen teko						
Vain muutama jäsen tekee päätöksiä.	1	2	3	4	5	Kaikki jäsenet ovat päätöksen teossa mukana.
Joustavuus						

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.

Ryhmä on lukkiutunut vakiintuneisiin sääntöihin ja proseduureihin, joita jäsenet näkevät vaikeaksi muuttaa.	1	2	3	4	5	Jäsenet ovat valmiina muuttamaan proseduureja tilanteen muuttuessa.
Jäsenten resurssien käyttö						
Yksilöiden kykyjä, tietoja ja kokemusta ei ole hyvin hyödynnetty.	1	2	3	4	5	Jokaisen jäsenen kyvyt, tiedot ja kokemus ovat täysin hyödynnettyjä.

Tämä projekti on rahoitettu Euroopan Komission tuella.
Tämä julkaisu ilmentää vain tekijöiden näkemyksiä ja Komissio ei ole vastuussa siitä, miten tämän julkaisun sisältämiä tietoja käytetään.