Nimi: _____ Päivämäärä: _____ Pisteet: _____

Tietosuoja ja yritysten tallennustila Tietoturvaopas

Tietojen maskaus, tokenisointi, levossa ja siirrossa olevan datan salaus, offline-varmuuskopiot

TIETOJEN SUOJAUKSEN OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: tietosuojastandardit ja valvontakeinot. Tutustut koko levyn salaukseen, suojattuihin käyttöoikeuksien hallintakeinoihin, laitteistovarmuuskopioihin, pilviturvallisuuden tilaan ja tietojen peittämistekniikoihin.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse kyberturvallisuus ja uhkien ehkäisy.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin kyberturvallisuusopas

URL: https://www.vpn.com/fi/kyberturvallisuus/tietojen-suojaaminen/

Oppimispolkusi: tietosuojastrategia

- Erota toisistaan tietojen maskaus- ja tokenisointitekniikat.
- Toteuta tallennusasemien salaus levossa ja siirrettävien tietojen salaus TLS:llä.
- Suunnittele offline-tilassa olevat, verkosta eristetyt varmuuskopiojärjestelmät kiristysohjelmasuojaukseen.

TIETOJEN SUOJAUKSEN OPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: tietosuoja. Lopuksi bonustehtävä Nopeat vastaukset.

TIETOJEN SUOJAUS JA YRITYSTALLENNUKSEN TURVALLISUUS (JOHDANTO)

Tietojen suojaus turvaa yrityksen tietovarat maskauksen, tokenisoinnin, levossa olevan tietokannan salauksen ja suojattujen siirtoprotokollien avulla. Verkosta eristettyjen varmuuskopioiden suunnittelu auttaa varmistamaan, että keskeiset tietokannat voidaan palauttaa käynnissä olevan tunkeutumisen sattuessa.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on tietojen maskauksen ensisijainen tarkoitus?

- A. Arkaluonteisten tunnisteiden korvaaminen fiktiivisillä mutta realistisilla merkeillä yksityisyyden suojaamiseksi
- B. Suurten tietokantatiedostojen pakkaaminen fyysisen palvelintilan säästämiseksi
- C. Vanhojen asiakkaiden yhteystietosähköpostien poistaminen arkistoivista varmuuskopiojärjestelmistä
- D. Tietokantapalvelimen julkisen IP-osoitteen piilottaminen internet-skannauksilta

2. Mikä mekanismi salaa tietokantapalvelimen kiintolevylle tallennetut tiedostot?

- A. Levyn täysi salaus lepotilassa
- B. TLS-istunnon kättelyprotokollat siirron aikana
- C. Dynaamisen DNS:n nimipalvelimien edelleenlähetyssäännöt
- D. Monivaiheinen todennus laitteistoavaimilla

3. Mikä edustaa siirrettävää dataa?

- A. Verkon reitittimien ja kytkimien kautta kulkevat datapaketit
- B. Tietokannan tapahtumalokit tallennettuna kylmälle varmuuskopiolevylle
- C. Arkistoidut käyttäjätiedostot, jotka on tallennettu eristettyyn pilviholviin
- D. Staattiset järjestelmän määritystiedostot paikallisessa pöytäkoneen tallennustilassa

4. Miksi säännöllinen offline-varmuuskopio on ratkaisevan tärkeä kiristysohjelmilta suojautumisessa?

- A. Se tarjoaa puhtaan, offline-kopion, jolla tiedostot voi palauttaa maksamatta lunnaita
- B. Se estää hakkereita skannaamasta avoimia porttimäärityksiä
- C. Se lisää paikallisen verkon tiedonsiirtonopeutta
- D. Se automatisoi evästesuostumuksen hyväksyntälokit selaimissa

5. Mitä tietojen tokenisointi tekee?

- A. Se korvaa arkaluonteiset korttinumerot ei-arkaluonteisilla satunnaisilla tunnuksilla
- B. Se reitittää verkkoliikenteen usean suojatun onion-solmun kautta
- C. Se skannaa järjestelmähakemistoja allekirjoituspohjaisten haittaohjelmien varalta
- D. Se auditoi tietokannan ylläpitäjien kirjautumisistuntojen kestoja

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Tietojen maskaus muuttaa tuotantoympäristöjen tietokantatietueita pysyvästi.

○ Tosi ○ Epätosi

7 Kysymys 7

7. Offsite-varmuuskopiot on eristettävä yrityksen pääverkosta kiristysohjelmien leviämisen estämiseksi.

○ Tosi ○ Epätosi

8 Kysymys 8

8. SSL/TLS-varmenteet suojaavat tietokantoja salaamalla fyysisellä medialla levossa olevan datan.

○ Tosi ○ Epätosi

9 Kysymys 9

9. Zero Trust Network Access (ZTNA) varmentaa jokaisen käyttäjän henkilöllisyyden ennen tietokantaan pääsyn myöntämistä.

○ Tosi ○ Epätosi

10 Kysymys 10

10. Holviin perustuva tokenisointi tallentaa alkuperäiset korttiarvot suojattuun keskitettyyn tokenholviin.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Henkilönimien korvaamista realistisilla paikkamerkeillä kutsutaan tietojen _____ .

2. Fyysisten tallennuslohkojen salaus suojaa tallennettuja tietokantaresursseja; tätä tilaa kutsutaan nimellä _____ .

3. TLS-protokollat salaavat aktiivisia datapaketteja, jotka liikkuvat tilassa nimeltä _____ .

4. Roolipohjaiset oikeudet rajaavat, millä käyttäjillä on tietokannan _____ .

5. Puhtaiden yritystiedostojen palauttaminen tietomurron jälkeen edellyttää turvallista offline-_____ .

6. Pilvikonfiguraatioiden auditointi arvioi organisaation tietoturvaa, jonka kokonaistilaa kutsutaan nimellä _____ .

SANASTON SANAPANKKI

KÄYTTÖOIKEUS LEPOTILA MASKAUS MINIMOINTI SIIRTO TIETOVUOTO TURVATILANNE VARMUUSKOPIO

Kirjoita vastauksesi tähän:

1.
2.
3.
4.
5.
6.

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

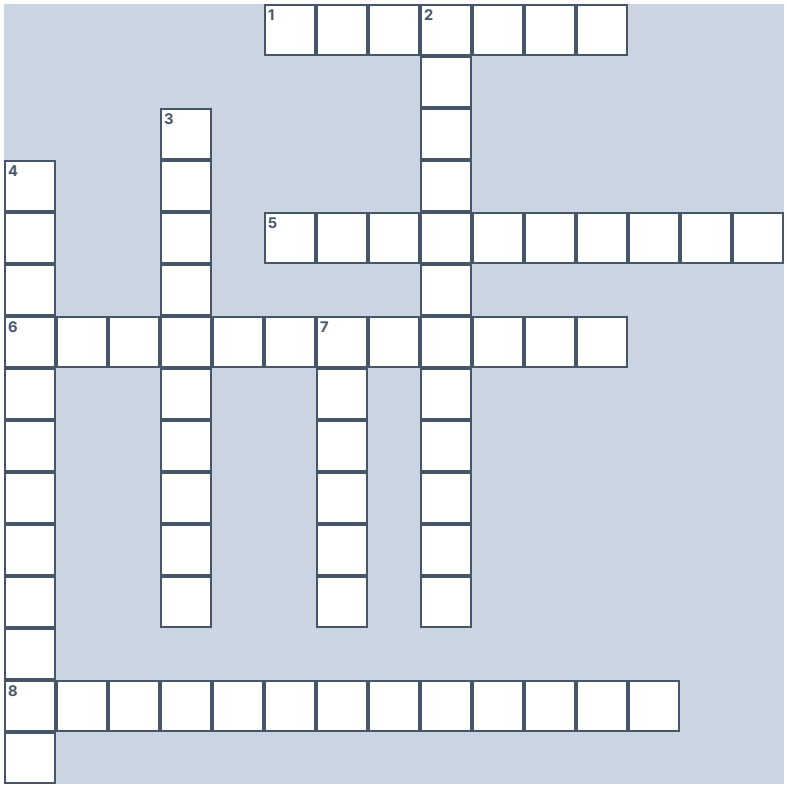
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. SALAUS	A	Turvallisten ulkopuolisten tietokopioiden luominen järjestelmävikojen varalta palautusta varten.
☐	2. VARMUUSKOPIO	B	Selkotekstin muuttaminen lukukelvottomaksi salatekstiksi, jotta siepattu data pysyy yksityisenä.
☐	3. MINIMOINTI	C	Organisaation pilven kokonaisvaltainen tietoturvatilanne ja puolustusvalmius.
☐	4. PÄÄSY	D	Säänteylystandardien, kuten GDPR:n tai CCPA:n, noudattaminen yksityisten käyttäjätietojen hallinnassa.
☐	5. LAITETILA	E	Tietoturvapoikkeama, jossa suojattuihin tietoihin päästään käsiksi tai ne paljastetaan luvatta.
☐	6. TIETOMURTO	F	Tietokannan luku- ja kirjoitusoikeuksien rajoittaminen todennetuille käyttäjärooleille.
☐	7. VAATIMUSTENMUKAISUUS	G	Arkaluonteisten merkkien korvaaminen tietokantakentissä henkilöllisyyksien suojaamiseksi.
☐	8. PEITTÄMINEN	H	Henkilötietojen keräämisen rajoittaminen toiminnan kannalta ehdottoman välttämättömään vähimmäismäärään.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

1. Arkaluonteisten merkkien korvaaminen tietokantakentissä henkilöllisyyksien suojaamiseksi. (7)

5. Tietoturvapoikkeama, jossa suojattuja tietoja käsitellään tai paljastetaan luvatta (10)

6. Tietojen suojattujen ulkopuolisten kopioiden luominen palautettavaksi järjestelmävikojen varalta. (12)

8. Sääntelystandardien, kuten GDPR:n tai CCPA:n, täyttäminen yksityisten käyttäjätietojen hallinnassa. (13)

PYSTYSUORAAN

2. Tietokannan luku- ja kirjoitusoikeuksien rajaaminen todennettuihin käyttäjärooleihin. (12)

3. Henkilötietojen keräämisen rajaaminen toiminnan kannalta ehdottomasti välttämättömään vähimmäismäärään. (10)

4. Organisaation pilven kokonaisvaltainen tietoturvatila ja puolustusvalmius. (12)

7. Selkotekstin muuntaminen lukukelvottomaksi salatekstiksi, jotta siepattu data pysyy yksityisenä (6)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin.

VAAKASUORAAN

1 vaakasuoraan: Arkaluonteisten merkkien korvaaminen tietokantakentissä henkilöllisyyksien suojaamiseksi. (7 kirjainta):

5 vaakasuoraan: Tietoturvapoikkeama, jossa suojattuja tietoja käsitellään tai paljastetaan luvatta (10 kirjainta):

6 vaakasuoraan: Tietojen suojattujen ulkopuolisten kopioiden luominen palautettavaksi järjestelmävikojen varalta. (12 kirjainta):

8 vaakasuoraan: Sääntelystandardien, kuten GDPR:n tai CCPA:n, täyttäminen yksityisten käyttäjätietojen hallinnassa. (13 kirjainta):

PYSTYSUORAAN

2 pystysuoraan: Tietokannan luku- ja kirjoitusoikeuksien rajaaminen todennettuihin käyttäjärooleihin. (12 kirjainta):

3 pystysuoraan: Henkilötietojen keräämisen rajaaminen toiminnan kannalta ehdottomasti välttämättömään vähimmäismäärään. (10 kirjainta):

4 pystysuoraan: Organisaation pilven kokonaisvaltainen tietoturvatila ja puolustusvalmius. (12 kirjainta):

7 pystysuoraan: Selkotekstin muuntaminen lukukelvottomaksi salatekstiksi, jotta siepattu data pysyy yksityisenä (6 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

O Ä K L X K Ä Y Å R L J Ö J K
I O A F J B V A K F Y F L Ö L
P E M S M I N I M O I N T I O
O K A G Q L P D O C D I J B B
K Q T N R Y W J Ä G Ä U H Å Z
S I F T W P W L T E V U N R M
U O U I L R I Ä Q N Z X P Ä S
U S E N N A L I T A V R U T B
M A M R O B M J G J P Ä C Ö Ö
R Ä B O Y Å N D S U A L A S F
A N O U D A T T A M I N E N Q
V Z R T I E T O V U O T O S Å
I E K Ä Y T T Ö O I K E U S Ä
C Z N F H I Ö Z D Q T L Z Å T
M Ö S U A K S A M A O T Ö T N

SANASTOLISTA

SALAUS VARMUUSKOPIO MINIMOINTI KÄYTTÖOIKEUS TURVATILANNE
TIETOVUOTO NOUDATTAMINEN MASKAUS

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. SALAUS**
- **B. VARMUUSKOPIO**
- **C. MINIMOINTI**
- **D. KÄYTTÖOIKEUS**
- **E. TURVATILANNE**
- **F. TIETOVUOTO**
- **G. NOUDATTAMINEN**
- **H. MASKAUS**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Tietoturvapoikkeama, jossa suojattuja tietoja käsitellään tai paljastetaan luvatta.
2. Arkaluonteisten merkkien korvaaminen tietokantakentissä henkilöllisyyksien suojaamiseksi.
3. Tietokannan luku- ja kirjoitusoikeuksien rajaaminen todennettuihin käyttäjärooleihin.
4. Organisaation pilven kokonaisvaltainen tietoturvatila ja puolustusvalmius.
5. Sääntelystandardien, kuten GDPR:n tai CCPA:n, täyttäminen yksityisten käyttäjätietojen hallinnassa.
6. Henkilötietojen keräämisen rajaaminen toiminnan kannalta ehdottomasti välttämättömään vähimmäismäärään.
7. Selkotekstin muuntaminen lukukelvottomaksi salatekstiksi, jotta siepattu data pysyy yksityisenä.
8. Tietojen suojattujen ulkopuolisten kopioiden luominen palautettavaksi järjestelmävikojen varalta.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä kyberturvallisuuden käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. LSAUSA
2. TIMIMIINON
3. TULINARTEANV
4. TEMUAANTNINOD
5. APKSORUOUVIM
6. STKEÖUIKÄOYT
7. ITTUVOTOOE
8. AKSMUAS

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Asioita, joista otat varmuuskopion			
2	Kyberturvallisuuteen liittyviä sanoja			
3	Ihmisiä, joilla on lupa nähdä arkaluonteisia tietoja			
4	Tapoja poistaa tietoja turvallisesti			
5	Paikkoja, joissa tietoja säilytetään			
6	Asioita, jotka pitäisi salata			
7	Tietoja, jotka sairaalan on suojattava			
8	Varmuuskopiotyyppejä			
9	Tietoja, joita sinun ei pitäisi koskaan jakaa			
10	Varoitusmerkkejä sähköpostissa			
11	Turvallisia tapoja, joita voit aloittaa tänään			
12	Ihmisiä, joilta voit pyytää IT-apua			
13	Laitteita, jotka voidaan hakkeroida			
14	Tapoja suojata tietoja			
15	Asioita, jotka voivat tuhota tietoja			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: YRITYSTIETOKANNAN LEPOTILAN SALAUKSEN PÄIVITYS

👷

Tilanne: Verkkokauppa tallentaa tapahtumatietokantoja pilvitallennustilaan ilman koko levyn salausta. Hiljattainen vaatimustenmukaisuustarkastus merkitsi tämän vakavaksi CCPA-tietoturvariskiksi. Suunnittele palautusarkkitehtuuri.

Keskustelukysymys: Analysoi CCPA-vaatimustenmukaisuusriskit ja ehdota levossa olevan datan salausstrategiaa.

TAPAUSTUTKIMUS 2: LUNNASOHJELMAN ERISTÄMINEN JA TIETOJEN PALAUTUS

👷

Tilanne: Aktiivinen kiristyshaittaohjelmahyökkäys salaa verkkolevyjä yrityksen paikallisverkossa. Ylläpitäjä on havainnut tartunnan varhain. Suunnittele eristys- ja palautusvaiheet.

Keskustelukysymys: Kuvaa välittömät eristystoimet ja suunnittele turvallinen palautusprosessi.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Kyberturvallisuuden ammattilainen suojaa verkon resursseja verkkohyökkääjiltä. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

19	21	15	10	1	1		25	11	19	9	20	25	9	19	5	20

20	9	5	4	15	20

8	1	12	12	9	14	20	1	11	5	9	14	15	9	12	12	1

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa A)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q1: Mitä on tietosuoja?

Se on henkilö- ja yritystietojen suojaamista luvattomalta käytöltä, katoamiselta tai vioittumiselta teknisin kontrollein.

Q2: Miksi koko levyn salaus on tärkeää?

Se suojaa fyysisillä levyillä olevat tallennetut datalohkot, jolloin kukaan ei voi lukea tietoja, vaikka varastaisi kiintolevyn fyysisesti.

Q3: Mikä on levossa olevan ja siirrettävän tiedon salauksen ero?

Levossa olevan datan salaus suojaa levyille tallennetut tiedostot, kun taas siirrossa olevan datan salaus suojaa reitittimien kautta kulkevat aktiiviset verkkopaketit.

Q4: Mitä tietojen maskaus on?

Se korvaa arkaluonteiset tiedot (kuten luottokorttinumerot) kuvitteellisilla mutta realistisilla tiedoilla testausta varten paljastamatta todellisia tietueita.

Q5: Miksi offline-varmuuskopio on tärkeä?

Se säilyttää puhtaan kopion tiedostoistasi eristettynä verkosta, mikä voi auttaa suojaamaan varmuuskopiosi kiristysohjelmien salaukselta.

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa B)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Mikä on tietojen tokenisointiholvi?

Suojattu, eristetty tietokanta, joka yhdistää satunnaiset tunnukset alkuperäisiin arkaluonteisiin arvoihinsa (kuten luottokorttien päänumeroihin).

Q7: Mitä Zero Trust -tietokantakäyttö tarkoittaa?

Se tarkoittaa jokaisen käyttäjän henkilöllisyyden ja laitteen tilan varmistamista jokaisella kirjautumisella sen sijaan, että kenenkään verkon sisällä olevan oletettaisiin olevan luotettava.

Q8: Miten TLS suojaa siirrettävää dataa?

TLS salaa TCP-istunnon hyötykuorman, mikä estää julkisten verkkojen haitallisia toimijoita nuuskimasta tai muokkaamasta siirrettäviä paketteja.

Q9: Mitä tietokantakäytön auditointi on?

Tietokantakyselyjen ja kirjautumisten jatkuva tallennus luvattoman käytön mallien tai tietoturvapoikkeamien havaitsemiseksi.

Q10: Mikä on pilvitietoturvan tilanteen tarkastus?

Prosessi, joka analysoi pilvimäärityksiä avoimien porttien, virheellisesti määritettyjen käyttösääntöjen ja tietoturvavaatimusten aukkojen tunnistamiseksi.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa C)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q1: Miten kirjekuorisalaus (envelope encryption) toimii?

Se salaa tiedot datavaimella ja salaa sitten datavaimen pääavaimella, mikä yksinkertaistaa avainten säilytystä ja kierrätystä.

Q2: Mitä on homomorfinen salaus?

Kehittynyt salausmenetelmä, jonka avulla toimintoja voidaan suorittaa suoraan salatulle datalle purkamatta sitä ensin.

Q3: Miksi tietokannassa käytetään sarakekohtaista salausta?

Se salaa tietyt arkaluonteiset sarakkeet (kuten henkilötunnukset) yksitellen ja suojaa ne, vaikka ylläpitäjät saisivat yleisen taulun lukuoikeuden.

Q4: Mitä tietovuotojen esto (DLP) on?

Ohjelmisto, joka valvoo verkon poistumispisteitä havaitakseen ja estääkseen arkaluonteisten tiedostojen luvattomat lähtevät siirrot.

Q5: Miten kerran kirjoitettavat, usein luettavat (WORM) varmuuskopiot suojaavat kiristyshaittaohjelmilta?

WORM-varmuuskopiot estävät tiedostojen poistamisen tai muuttamisen tietyn ajan, jolloin kiristysohjelma ei voi salata olemassa olevia varmuuskopioita.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa D)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q6: Mikä on avainten uudelleenkäytön riski?

Saman salausavaimen käyttäminen eri tietokannoissa tarkoittaa, että yhden avaimen vaarantuminen paljastaa kaikki tietokannat.

Q7: Miten tietokannan tokenisointi parantaa CCPA-vaatimustenmukaisuutta?

Tokenit pseudonymisoivat tietueet tuotannon ulkopuolisissa järjestelmissä ja rajoittavat tietomurron vaikutusta, mutta tokenoitu data voi silti olla henkilötietoa.

Q8: Miksi tietojen luokittelu on kriittistä?

Se luokittelee tiedostot herkkyystason mukaan ja auttaa organisaatioita soveltamaan vahvimman salauksen ja käyttöoikeuksien hallinnan korkean riskin tietoihin.

Q9: Mikä rooli avainten kierrolla on?

Salausavainten säännöllinen päivittäminen rajoittaa altistuvan historiallisen datan määrää, jos yksittäinen avain murretaan myöhemmin.

Q10: Miten suojatut enklaavit suojaavat tietokantakyselyjä muistissa?

Suojatut enklaavit eristävät kyselytoiminnot suorittimen suojattuihin muistilohkoihin, mikä estää isäntäjärjestelmän ylläpitäjiä näkemästä selkotekstiä RAM-muistissa.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

GDPR-säännökset tulivat voimaan toukokuussa 2018, ja ne muuttivat tapaa, jolla maailmanlaajuiset sivustot hallinnoivat evästesuostumuksia ja henkilötietorekistereitä.

2. TURVALLISUUSOIVALLUS

GDPR-rikkomuksen sakko voi nousta 20 miljoonaan euroon tai 4 prosenttiin maailmanlaajuisesta liikevaihdosta, mikä merkitsee huomattavaa oikeudellista riskiä. [4]

3. TURVALLISUUSOIVALLUS

CCPA tuli voimaan tammikuussa 2020, ja se loi Yhdysvalloissa uranuurtavat kuluttajien digitaalisen yksityisyyden oikeudet.

4. TURVALLISUUSOIVALLUS

Tietojen minimointi pienentää tietokannan tallennustilan tarvetta, mikä alentaa palvelinten käyttökustannuksia ja pienentää tietomurron vaikutuksia.

5. TURVALLISUUSOIVALLUS

Kryptografinen tuhoaminen ratkaisee varmuuskopioiden poiston haasteen poistamalla avaimia sen sijaan, että historiallisia varmuuskopionauhatiedostoja muokattaisiin.

6. TURVALLISUUSOIVALLUS

Useimmat maat ympäri maailmaa ovat nykyään säätäneet henkilötietojen suojaa koskevia lakeja kuluttajien yksityisyysoikeuksien turvaamiseksi.

7. TIETOTURVATIETOA

Valmiiksi rastitetut suostumuslomakkeet on nimenomaisesti kielletty Euroopan tietosuojasääntelyn määritelmien mukaan.

8. TIETOTURVATIETOA

GDPR edellyttää henkilötietojen tietoturvaloukkausten ilmoittamista valvontaviranomaiselle 72 tunnin kuluessa tietoon saamisesta, jos se on mahdollista. [3]

9. TIETOTURVATIETOA

Salasanojen tiivistäminen hitailla algoritmeilla, kuten bcryptillä tai Argon2:lla, vaikeuttaa huomattavasti varastettujen tiivisteiden murtamista offline-tilassa. [6]

10. TURVALLISUUSOIVALLUS

Levossa oleva data tarkoittaa tallennettuja tietokantatiedostoja, kun taas siirrossa oleva data kattaa verkon reitittimien läpi aktiivisesti kulkevat paketit.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista.

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on tietojen maskauksen ensisijainen tarkoitus? → Arkaluonteisten tunnisteiden korvaaminen fiktiivisillä mutta realistisilla merkeillä yksityisyyden suojaamiseksi

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mikä mekanismi salaa tietokantapalvelimen kiintolevylle tallennetut tiedostot? → Levyn täysi salaus lepotilassa

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä edustaa siirrettävää dataa? → Verkon reitittimien ja kytkimien kautta kulkevat datapaketit

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Miksi säännöllinen offline-varmuuskopio on ratkaisevan tärkeä kiristysohjelmilta suojautumisessa? → Se tarjoaa puhtaan, offline-kopion, jolla tiedostot voi palauttaa maksamatta lunnaita

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mitä tietojen tokenisointi tekee? → Se korvaa arkaluonteiset korttinumerot ei-arkaluonteisilla satunnaisilla tunnuksilla

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 Kysymys 6

Oikea vastaus: Epätosi

OPETTAJALLE

Maskaus muuttaa testikopioita tai piilottaa arvot kyselyhetkellä; tuotantotietueet pysyvät muuttumattomina.

7 Kysymys 7

Oikea vastaus: Tosi

OPETTAJALLE

Offsite-varmuuskopiot on eristettävä yrityksen pääverkosta kiristysohjelmien leviämisen estämiseksi.

8 Kysymys 8

Oikea vastaus: Epätosi

OPETTAJALLE

TLS-varmenteet suojaavat siirrettävää dataa; levossa oleva data tarvitsee levy-, tiedosto- tai tietokantasalauksen.

9 Kysymys 9

Oikea vastaus: Tosi

OPETTAJALLE

Zero Trust Network Access (ZTNA) varmentaa jokaisen käyttäjän henkilöllisyyden ennen tietokantaan pääsyn myöntämistä.

10 Kysymys 10

Oikea vastaus: Tosi

OPETTAJALLE

Holviin perustuva tokenisointi säilyttää alkuperäiset arvot suojatussa tokenholvissa, joka yhdistää jokaisen tokenin takaisin sen dataan.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

B 1. SALAUS	A 2. VARMUUSKOPIO	H 3. MINIMOINTI	F 4. PÄÄSY
C 5. LAITETILA	E 6. TIETOMURTO	D 7. VAATIMUSTENMUKAISUUS	G 8. PEITTÄMINEN

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 MASKAUS	2 LEPOTILA	3 SIIRTO	4 KÄYTTÖOIKEUS
5 VARMUUSKOPIO	6 TURVATILANNE		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 F – TIETOVUOTO	2 H – MASKAUS	3 D – KÄYTTÖOIKEUS	4 E – TURVATILANNE
5 G – NOUDATTAMINEN	6 C – MINIMOINTI	7 A – SALAUS	8 B – VARMUUSKOPIO

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit SALAUS, VARMUUSKOPIO ja MINIMOINTI omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

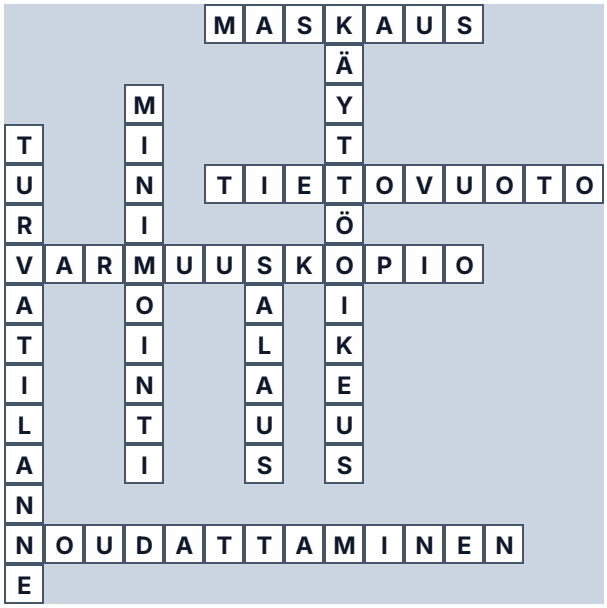
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

O	Ä	K	L	X	K	Ä	Y	Å	R	L	J	Ö	J	K
I	O	A	F	J	B	V	A	K	F	Y	F	L	Ö	L
P	E	M	S	M	I	N	I	M	O	I	N	T	I	O
O	K	A	G	Q	L	P	D	O	C	D	I	J	B	B
K	Q	T	N	R	Y	W	J	Ä	G	Ä	U	H	Å	Z
S	I	F	T	W	P	W	L	T	E	V	U	N	R	M
U	O	U	I	L	R	I	Ä	Q	N	Z	X	P	Ä	S
U	S	E	N	N	A	L	I	T	A	V	R	U	T	B
M	A	M	R	O	B	M	J	G	J	P	Ä	C	Ö	Ö
R	Ä	B	O	Y	Å	N	D	S	U	A	L	A	S	F
A	N	O	U	D	A	T	T	A	M	I	N	E	N	Q
V	Z	R	T	I	E	T	O	V	U	O	T	O	S	Å
I	E	K	Ä	Y	T	T	Ö	O	I	K	E	U	S	Ä
C	Z	N	F	H	I	Ö	Z	D	Q	T	L	Z	Å	T
M	Ö	S	U	A	K	S	A	M	A	O	T	Ö	T	N

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

1 vaakasuoraan: MASKAUS Arkaluonteisten merkkien korvaaminen tietokantakentissä henkilöllisyyksien suojaamiseksi. (7 kirjainta)

5 vaakasuoraan: TIETOVUOTO Tietoturvapoikkeama, jossa suojattuja tietoja käsitellään tai paljastetaan luvatta (10 kirjainta)

6 vaakasuoraan: VARMUUSKOPIO Tietojen suojattujen ulkopuolisten kopioiden luominen palautettavaksi järjestelmävikojen varalta. (12 kirjainta)

8 vaakasuoraan: NOUDATTAMINEN Sääntelystandardien, kuten GDPR:n tai CCPA:n, täyttäminen yksityisten käyttäjätietojen hallinnassa. (13 kirjainta)

PYSTYSUORAAN

2 pystysuoraan: KÄYTTÖOIKEUS Tietokannan luku- ja kirjoitusoikeuksien rajaaminen todennettuihin käyttäjärooleihin. (12 kirjainta)

3 pystysuoraan: MINIMOINTI Henkilötietojen keräämisen rajaaminen toiminnan kannalta ehdottomasti välttämättömään vähimmäismäärään. (10 kirjainta)

4 pystysuoraan: TURVATILANNE Organisaation pilven kokonaisvaltainen tietoturvatila ja puolustusvalmius. (12 kirjainta)

7 pystysuoraan: SALAUS Selkotekstin muuntaminen lukukelvottomaksi salatekstiksi, jotta siepattu data pysyy yksityisenä (6 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. LSAUSA — **SALAUS**
2. TIMIMIINON — **MINIMOINTI**
3. TULINARTEANV — **TURVATILANNE**
4. TEMUAANTNINOD — **NOUDATTAMINEN**
5. APKSORUOUVIM — **VARMUUSKOPIO**
6. STKEÖUIKÄOYT — **KÄYTTÖOIKEUS**
7. ITTUVOTOOE — **TIETOVUOTO**
8. AKSMUAS — **MASKAUS**

SALAKIRJOITUSHAASTEEN AVAIN

"SUOJAA YKSITYISET TIEDOT HALLINTAKEINOILLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Yritystietokannan lepotilan salauksen päivitys

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Verkkokauppa tallentaa tapahtumatietokantansa pilvitallennustilaan ilman koko levyn salausta. Hiljattainen vaatimustenmukaisuustarkastus merkitsi tämän vakavaksi CCPA-tietoturvariskiksi. Suunnittele palautusarkkitehtuuri.
- Suositeltu strategia ja ratkaisu: Ota käyttöön AES-256-levysalaus kaikissa tiedostojärjestelmissä. Käytä keskitettyä avainhallintapalvelua (KMS) automaattisella avainkierrolla ja pakota tiukat IAM-käytännöt purkuoikeuksien hallintaan.

B Tapaustutkimus 2: Lunnasohjelman eristäminen ja tietojen palautus

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Aktiivinen kiristysohjelmahyökkäys salaa verkkoasemia yrityksen lähiverkossa. Ylläpitäjä on havainnut tartunnan varhain. Suunnittele rajaamis- ja palautusvaiheet.
- Suositeltu strategia ja ratkaisu: Eristä vaarantunut verkon osa välittömästi. Alusta vaikutuksen kohteena olevat päätelaitteet ja palauta tiedot viimeisimmästä offline-tilassa olevasta kertakirjoitteisesta (WORM) varmuuskopiosta. Varmista varmuuskopion eheys ennen järjestelmien yhdistämistä takaisin.