

Irányítópult / Kurzusok / 2022/23/2 / NIK

/ 2022/23/2 - Bevezetés a kiberbiztonságba - biztonságtudatosság - NBXKB1HMNE/BevKib_EA_SOC / 14. ZH

/ Bevezetés a kiberbiztonságba - biztonságtudatosság ZH

Kezdés ideje	2023. május 26., péntek, 17:05
Állapot	Befejezte
Befejezés dátuma	2023. május 26., péntek, 17:46
Felhasznált idő	40 perc 40 mp
Pont	50,83 a(z) 55,00 maximumból (92%)

1 kérdés

Helyes

1,00/1,00 pont

Az adatmanipuláció napjainkban egyre kevesebb veszélyt jelent lévén annak, hogy a kiberbiztonsági megoldások egyre korszerűbbek.

Válasszon ki egyet:

- ☐ Igaz
- ☒ Hamis ✓

A helyes válasz a 'Hamis'.

2 kérdés

Helyes

1,00/1,00 pont

Jelölje be azt az állítást az OSINT-al kapcsolatban mely hamis:

Válasszon ki egyet:

- ☐ Nyílt forrású hírszerzésként is emlegetik,
- ☒ Az internet létrejötte előtt nem létezett. ✓
- ☐ Léteznek olyan AI-ok melyek segítenek az OSINT-ba.
- ☐ Az OSINT alapvetően legális.

Válasza helyes.

A helyes válasz:

Az internet létrejötte előtt nem létezett..

Weboldal

Help

Donate

✖

757 tárgy, 161 506 kérdés

qmining.joesrv.net:443

1,00/1,00 pont

Felhasználói profilalkotást a közösségi médiában, csak az oldal üzemeltetője végez.

Válasszon ki egyet:

☒ Igaz ✓

☐ Hamis

A helyes válasz az 'Igaz'.

4 kérdés

Helyes

1,00/1,00 pont

Előfordulhat, hogy egy rendszer felé irányuló trollkodásnak felhasználók is áldozatává válnak.

Válasszon ki egyet:

☒ Igaz ✓

☐ Hamis

A helyes válasz az 'Igaz'.

5 kérdés

Helyes

1,00/1,00 pont

Az internetes zaklatás akár bűnszervezetek „alapozó” eszköze is lehet.

Válasszon ki egyet:

☒ Igaz ✓

☐ Hamis

A helyes válasz az 'Igaz'.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

A BCP tesztelés során nincs szükség dedikált döntéshozói szerepekre, hiszen mindenki tudja, hogy mi a dolga egy leállás esetén.

Válasszon ki egyet:

- ☐ Igaz
- ☒ Hamis ✓

A helyes válasz a 'Hamis'.

7 kérdés

Helyes

1,00/1,00 pont

Jelölje be a BCP életciklus összes tevékenységét

Válasszon ki egyet vagy többet:

- ☒ Kockázat felmérés ✓
- ☒ Üzleti hatáselemzés ✓
- ☐ Redundáns szerverpark kialakítása
- ☒ BCP stratégia kiválasztása ✓
- ☒ BCP és DRP tervek kialakítása ✓
- ☒ Oktatás, tesztelés, karbantartás ✓
- ☐ Kockázatkezelési intézkedési terv elkészítése

Válasza helyes.

A helyes válaszok: Kockázat felmérés,

Üzleti hatáselemzés,

BCP stratégia kiválasztása,

BCP és DRP tervek kialakítása,

Oktatás, tesztelés, karbantartás

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

0,00/1,00 pont

Jelölje be, hogy melyik állítás nem igaz az üzleti hatáselemzésre (BIA)

Válasszon ki egyet vagy többet:

- ☒ Célja, hogy meghatározza a leállás által okozott kárt ✖
- ☐ Műszaki elemzés, az IT terület bevonásával történik a kárbecslés
- ☒ Minden üzleti folyamathoz meghatározza az MTD értékeket ✖
- ☒ Meghatározza, hogy az MTD-n túli leállás naponta, hetente stb. mekkora kárt okoz ✖
- ☐ A leállások hatását minden esetben kvalitatív módszerrel határozza meg
- ☒ Interjúk módszerrel történik a felmérés ✖

Válasza helytelen.

A helyes válaszok:

Műszaki elemzés, az IT terület bevonásával történik a kárbecslés,

A leállások hatását minden esetben kvalitatív módszerrel határozza meg

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Írja be az állítás mellé annak a folyamatnak a betűjelét, amelyekre igaz:

Alternatív üzleti folyamatok: A

DRP visszaállítási lépések: D

Proaktív megközelítés	A	✓
Reaktív megközelítés	D	✓
Az IT rendszer leállása esetére leírja, hogy hogyan kell végezni a munkát	A	✓
Leírja, hogyan kell az IT rendszert a meghatározott idő alatt visszaállítani	D	✓
Technológia fókuszú megközelítés	D	✓
Rendszeres tesztelés szükséges	A, D	✓
Biztosítja, hogy a leállás alatt se álljanak a kritikus folyamatok	A	✓
Holisztikus, vállalati fókuszú	A	✓

Válasza helyes.

A helyes válasz:

Proaktív megközelítés → A,

Reaktív megközelítés → D,

Az IT rendszer leállása esetére leírja, hogy hogyan kell végezni a munkát → A,

Leírja, hogyan kell az IT rendszert a meghatározott idő alatt visszaállítani → D,

Technológia fókuszú megközelítés → D,

Rendszeres tesztelés szükséges → A, D,

Biztosítja, hogy a leállás alatt se álljanak a kritikus folyamatok → A,

Holisztikus, vállalati fókuszú → A

Weboldal

Help

Donate



757 tárgy, 161 506 kérdés

MOODLE | ÓBUDAI EGYETEM

Kérdések elküldve, katt az elküldő

0,50/1,00 pont

Írja be az állítás mellé annak a mentési típusnak a betűjelét, amelyikre igaz:

Teljes mentés: T

Inkrementális mentés: I

Differenciális mentés: D

Folyamatos mentés: F

Mindig mindent mentünk. Leginkább tárhely igényes

T



Mindig az előző teljes mentés óta megváltozott fájlokat mentjük

I



Mindig az előző mentés óta megváltozott fájlokat mentjük

D



Minden adatváltozást azonnal lementünk

F



Válasza részben helyes.

Jól választott ki: 2.

A helyes válasz:

Mindig mindent mentünk. Leginkább tárhely igényes → T,

Mindig az előző teljes mentés óta megváltozott fájlokat mentjük → D,

Mindig az előző mentés óta megváltozott fájlokat mentjük → I,

Minden adatváltozást azonnal lementünk → F

11 kérdés

Helyes

1,00/1,00 pont

Mi az a GDPR, és mire használjuk?

Válasszon ki egyet:

- ☒ Adatvédelmi irányelv az Európai Unióban ✓
- ☐ Személyes adatok gyűjtésére és tárolására szolgáló szoftver
- ☐ Közösségi oldal, amelyet az adatok védelmének céljából hoztak létre

Válasza helyes.

A helyes válasz:

Adatvédelmi irányelv az Európai Unióban.

Weboldal

Help

Donate



757 tárgy, 161 506 kérdés

1,00/1,00 pont

Ki számít az adatkezelőnek a GDPR értelmében?

Válasszon ki egyet:

- ☐ Az a személy vagy szervezet, aki/amely az adatokat előállítja
- ☒ Az a személy vagy szervezet, aki/amely a személyes adatokat kezeli és felelős azok védelméért ✓
- ☐ Az a személy vagy szervezet, aki/amely az adatokat elosztja a felhasználók között

Válasza helyes.

A helyes válasz:

Az a személy vagy szervezet, aki/amely a személyes adatokat kezeli és felelős azok védelméért.

13 kérdés

Helyes

1,00/1,00 pont

Milyen jogai vannak az érintetteknek a GDPR szerint?

Válasszon ki egyet:

- ☒ Hozzáférés, helyesbítés, törlés, adathordozhatóság, tiltakozás ✓
- ☐ Adatgyűjtés, adatkezelés, adatátvitel
- ☐ Adatfeldolgozás, adatvédelem, adatbiztonság

Válasza helyes.

A helyes válasz:

Hozzáférés, helyesbítés, törlés, adathordozhatóság, tiltakozás.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

0,67/1,00 pont

Milyen adatokat kell az adatkezelőnek védenie a GDPR szerint?

Válasszon ki egyet vagy többet:

- ☒ Személyazonossági adatok, egészségügyi adatok, vallási meggyőződés ✓
- ☒ Életkor, nem, lakhely ✓
- ☐ Banki információk, számlaadatok, jelszavak

Válasza részben helyes.

Jól választott ki: 2.

A helyes válaszok:

Személyazonossági adatok, egészségügyi adatok, vallási meggyőződés,

Életkor, nem, lakhely,

Banki információk, számlaadatok, jelszavak

15 kérdés

Helyes

1,00/1,00 pont

A felfedezésétől számítva mennyi idő elteltével kell értesíteni az érintetteket adatvédelmi incidens esetén a GDPR szerint?

Válasszon ki egyet:

- ☒ Azonnal, legkésőbb 72 órán belül ✓
- ☐ 1 héten belül
- ☐ A következő hónapban

Válasza helyes.

A helyes válasz:

Azonnal, legkésőbb 72 órán belül.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Mit kell tenni, ha valamelyik jelszavunk kompromittálódott?

Válasszon ki egyet:

- ☐ Semmit, mert már megtörtént a baj
- ☒ Azonnal változtassuk meg a jelszavunkat minden olyan helyen, ahol ugyanaz vagy hasonló jelszót használtunk ✓
- ☐ Várjunk, amíg a szolgáltató javasol valamit

Válasza helyes.

A helyes válasz:

Azonnal változtassuk meg a jelszavunkat minden olyan helyen, ahol ugyanaz vagy hasonló jelszót használtunk.

17 kérdés

Helyes

1,00/1,00 pont

Hogyan lehet megakadályozni a jelszavaink elvesztését?

Válasszon ki egyet:

- ☐ Az összes jelszó egy számítógépes adathordozón történő tárolásával, amit mindig magunknál tartunk
- ☐ Az összes jelszó papíron történő tárolásával, amit mindig magunknál tartunk
- ☒ Használjunk jelszómenedzsert, hogy biztonságosan tároljuk és könnyen elérjük az összes jelszavunkat ✓

Válasza helyes.

A helyes válasz:

Használjunk jelszómenedzsert, hogy biztonságosan tároljuk és könnyen elérjük az összes jelszavunkat.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Mi a legfontosabb dolog, amit meg kell tennünk a jelszavaink biztonságának biztosítása érdekében?

Válasszon ki egyet vagy többet:

- ☒ A jelszavaink sok karakterből álljanak: tartalmazzanak betűt, számot és akár speciális karaktert is ✓
- ☒ Időről időre változtassuk meg a jelszavainkat ✓
- ☒ Használjunk különböző jelszavakat minden hozzáférésünkhöz, és soha ne osszuk meg őket másokkal. ✓

Válasza helyes.

A helyes válaszok:

A jelszavaink sok karakterből álljanak: tartalmazzanak betűt, számot és akár speciális karaktert is,

Időről időre változtassuk meg a jelszavainkat,

Használjunk különböző jelszavakat minden hozzáférésünkhöz, és soha ne osszuk meg őket másokkal.

19 kérdés

Helyes

1,00/1,00 pont

Melyik a legerősebb jelszó az alábbiak közül?

Válasszon ki egyet:

- ☐ "password"
- ☐ "12345678"
- ☒ "jW\$e9@5L" ✓

Válasza helyes.

A helyes válasz:

"jW\$e9@5L".

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Mi az a kétlépcsős azonosítás, és miért hasznos?

Válasszon ki egyet:

- ☒ A jelszó mellett egy második védelmi réteg (pl. SMS-ben érkező kód) hozzáadása. Ezzel megnehezítjük a hackertámadásokat. ✓
- ☐ Két különböző jelszó használata minden hozzáféréshez, hogy megakadályozzuk az illetéktelen hozzáférést.
- ☐ Az összes jelszó feljegyzése egy helyen, hogy könnyebben hozzáférjünk.

Válasza helyes.

A helyes válasz:

A jelszó mellett egy második védelmi réteg (pl. SMS-ben érkező kód) hozzáadása. Ezzel megnehezítjük a hackertámadásokat..

21 kérdés

Helyes

1,00/1,00 pont

Mi a Social Engineering?

Válasszon ki egyet:

- ☐ Egy speciális vírusprogram
- ☒ Az emberek bizalomra való hajlamának felhasználása védett információ megszerzéséhez ✓
- ☐ Egy támadási módszer, amely fizikai erőszakot használ

Válasza helyes.

A helyes válasz:

Az emberek bizalomra való hajlamának felhasználása védett információ megszerzéséhez.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Milyen célja van a Social Engineering támadásoknak?

Válasszon ki egyet vagy többet:

- ☒ Adathalászat ✓
- ☒ Adatlopás ✓
- ☒ Információgyűjtés egy későbbi időpontban elkövetett, számítógépes eszközökkel történő támadás elősegítéséhez ✓

Válasza helyes.

A helyes válaszok:

Adathalászat,

Adatlopás,

Információgyűjtés egy későbbi időpontban elkövetett, számítógépes eszközökkel történő támadás elősegítéséhez

23 kérdés

Helyes

1,00/1,00 pont

Mi a leggyakoribb Social Engineering módszer?

Válasszon ki egyet:

- ☐ Nyitott portok felderítése
- ☐ Álhírek terjesztése
- ☒ A felhasználó bizalmának megszerzése ✓

Válasza helyes.

A helyes válasz:

A felhasználó bizalmának megszerzése.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Mi a "phishing" támadás?

Válasszon ki egyet:

- ☒ Hamis weboldalak, megtévesztő e-mail-ek használata az adatok ellopásához ✓
- ☐ Vírusok elhelyezése a felhasználó számítógépén
- ☐ A fizikai erőszak alkalmazása az adatok megszerzéséhez

Válasza helyes.

A helyes válasz:

Hamis weboldalak, megtévesztő e-mail-ek használata az adatok ellopásához.

25 kérdés

Helyes

1,00/1,00 pont

Milyen módon védheti meg magát a "phishing" támadásoktól?

Válasszon ki egyet vagy többet:

- ☒ Soha ne osszon meg érzékeny személyes adatokat az interneten ✓
- ☒ Ellenőrizze a webhelyek hitelességét és SSL tanúsítványát ✓
- ☒ Járjon el körültekintően az e-mailek megnyitásakor, különös tekintettel a csatolmányokra és a levélben szereplő linkekre ✓

Válasza helyes.

A helyes válaszok:

Soha ne osszon meg érzékeny személyes adatokat az interneten,

Ellenőrizze a webhelyek hitelességét és SSL tanúsítványát,

Járjon el körültekintően az e-mailek megnyitásakor, különös tekintettel a csatolmányokra és a levélben szereplő linkekre

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Mi az az ACL?

Válasszon ki egyet:

- ☒ Access Control List: meghatározza, hogy egy adott objektumhoz ki férhet hozzá vagy milyen műveleteket lehet végrehajtani. ✓
- ☐ Access Control List: mely meghatározza, hogy egy felhasználó milyen dokumentumokhoz férhet hozzá.
- ☐ Access Configuration List: Tartalmazza, hogy a felhasználók milyen erőforrásokhoz férhetnek hozzá.
- ☐ Access Certification List: Meghatározza, milyen szintű jogosultsággal lehet hozzáférni az objektumhoz.

Válasza helyes.

A helyes válasz:

Access Control List: meghatározza, hogy egy adott objektumhoz ki férhet hozzá vagy milyen műveleteket lehet végrehajtani..

27 kérdés

Helyes

1,00/1,00 pont

Mi az az RBAC?

Válasszon ki egyet:

- ☐ Role Based Access Control: meghatározza, hogy milyen szerepkörben lehetséges egy dokumentumon műveletet végezni.
- ☐ Rule Based Access Control: meghatározza, hogy milyen szabályok alapján lehet hozzáférni egy objektumhoz.
- ☒ Mindkettő ✓
- ☐ Egyik sem.

Válasza helyes.

A helyes válasz:

Mindkettő.

Weboldal

Help

Donate



757 tárgy, 161 506 kérdés

1,00/1,00 pont

Hogyan védettek a Kerberos protokoll üzenetei a lehallgatások ellen?

Válasszon ki egyet:

- ☐ Az tokenek továbbítása nem informatikai hálózaton keresztül történik.
- ☒ Az üzeneteket szimmetrikus kulcsú titkosítással védi a protokoll. ✓
- ☐ A kerberos egy hálózati hitelesítési protokoll, és az üzenetek nem férhetők hozzá a számítógépeken.
- ☐ A kerberos protokoll tervezése miatt, az azonosító tokenek elosztottak a hálózaton, egy időben egy helyen nem találhatók meg.

Válasza helyes.

A helyes válasz:

Az üzeneteket szimmetrikus kulcsú titkosítással védi a protokoll..

29 kérdés

Helyes

1,00/1,00 pont

Az LDAP egy:

Válasszon ki egyet:

- ☒ Lightweight Directory Access Protocol, amely hálózati szolgáltatások elérését szabályozza. ✓
- ☐ Light Director Protocol: egy számítógép távoli hozzáférését implementálja.
- ☐ Lightweight Directory Protocol: egyszerűsített hozzáférés-vezérlő alkalmazás.
- ☐ Lightweight Directory Access: könyvtárak távoli elérését szabályozó alkalmazás.

Válasza helyes.

A helyes válasz:

Lightweight Directory Access Protocol, amely hálózati szolgáltatások elérését szabályozza..

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

0,00/1,00 pont

A Bell-Lapadula modell olyan hozzáférés-vezérlési elvet ír le, ahol:

Válasszon ki egyet:

- ☐ Biztonsági címkéket használnak az objektumokon és engedélyeket az alanyok számára.
- ☐ Információs integritás fogalmának formalizálására irányul.
- ☒ A modell biztonsági címkéket használ, hogy hozzáférést biztosítson az objektumokhoz átalakítási eljárásokon és egy korlátozott interfész modellen keresztül. ✖
- ☐ Egy identitásszolgáltató (IdP) és egy szolgáltató (SP) között XML-alapú nyílt szabványú kommunikációval történik az identitásadatok átvitelére két fél között.

Válasza helytelen.

A helyes válasz:

Biztonsági címkéket használnak az objektumokon és engedélyeket az alanyok számára..

31 kérdés

Részben helyes

0,67/1,00 pont

Az alábbiak közül melyek tekinthetők technikai kontrollnak?

Válasszon ki egyet vagy többet:

- ☒ Hálózatba integrált tűzfal ✓
- ☐ Hálózati forgalmat megfigyelő IDS
- ☐ Levelezőrendszerbe integrált vírusvédelem
- ☒ Megkerülhetetlen Proxy kijárat ✓

Válasza részben helyes.

Jól választott ki: 2.

A helyes válaszok:

Hálózatba integrált tűzfal,

Levelezőrendszerbe integrált vírusvédelem,

Megkerülhetetlen Proxy kijárat

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Az alábbiak közül melyek tekinthetők adminisztratív kontrollnak?

Válasszon ki egyet vagy többet:

- ☐ Szabályrendszer, mely meghatározza a hálózati routeingot.
- ☒ Szabályrendszer, mely leírja a belépőkártya használatát ✓
- ☒ E-mail alapú tudatosító kampány ✓
- ☒ Biztonsági konfiguráció dokumentációja ✓

Válasza helyes.

A helyes válaszok:

Szabályrendszer, mely leírja a belépőkártya használatát,

E-mail alapú tudatosító kampány,

Biztonsági konfiguráció dokumentációja

33 kérdés

Helyes

1,00/1,00 pont

Az APT-k miért kiemelten veszélyes támadások?

Válasszon ki egyet:

- ☐ Mert a támadás során fedettek maradnak az elkövetők.
- ☐ Mert a támadásra való felkészülés időben rövidebb, mint a feltárt sérülékenységek kihasználásának ideje.
- ☒ Mert a betörés és a valós adatlopás, károkozás között akár több hónap is eltelhet. ✓
- ☐ Mert nem lehet tudni, honnan aktiválják az támadást.

Válasza helyes.

A helyes válasz:

Mert a betörés és a valós adatlopás, károkozás között akár több hónap is eltelhet..

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Melyik OSI szinten lehet azonosítani egy webes sérülékenységet kihasználó támadást?

Válasszon ki egyet:

- ☐ 3. Transport Layer
- ☐ 1. Physical layer
- ☒ 7. Application layer ✓
- ☐ 5. Session layer

Válasza helyes.

A helyes válasz:

7. Application layer.

35 kérdés

Helyes

1,00/1,00 pont

Az alábbiak közül melyek szerepelnek évek óta az OWASP top 10-ben, mint legtöbbször kihasznált webes sérülékenység?

Válasszon ki egyet:

- ☐ Cross Site Request Forgery (CSRF)
- ☒ Cross Site Scripting (XSS) ✓
- ☐ Insecure Communication
- ☐ Insufficient Logging and Monitoring

Válasza helyes.

A helyes válasz:

Cross Site Scripting (XSS).

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Tudatosság az a képesség, melyben közvetlenül megismerjük és érzékeljük az eseményeket. Olyan állapot, amelyben:

Válasszon ki egyet vagy többet:

- ☒ az alany bír valamilyen információval ✓
- ☒ ez az információ rendelkezésére áll ✓
- ☒ és amely befolyásolja viselkedési folyamatait ✓
- ☐ tudatos a hozzáállás. ✗

Válasza helyes.

A helyes válaszok:

az alany bír valamilyen információval,

ez az információ rendelkezésére áll,

és amely befolyásolja viselkedési folyamatait

37 kérdés

Helyes

1,00/1,00 pont

A biztonság-tudatosság arra összpontosít, hogy

Válasszon ki egyet vagy többet:

- ☒ tudatosítsa a gyorsan változó információs formák lehetséges kockázatait ✓
- ☒ az információ gyorsan növekvő veszélyeit ✓
- ☒ amelyek az emberi viselkedést célozzák meg ✓
- ☐ biztonságos kapcsolatot teremtsen az emberek és a gépek között.

Válasza helyes.

A helyes válaszok:

tudatosítsa a gyorsan változó információs formák lehetséges kockázatait,

az információ gyorsan növekvő veszélyeit,

amelyek az emberi viselkedést célozzák meg

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Az ENISA top 15 fenyegetésének listáján melyik támadás célpontja az ember?

Válasszon ki egyet vagy többet:

- ☒ Adathalászat ✓
- ☒ Spam ✓
- ☒ Személyiség lopás ✓
- ☐ Webes támadás

Válasza helyes.

A helyes válaszok:

Adathalászat,

Spam,

Személyiség lopás

39 kérdés

Helyes

1,00/1,00 pont

Az ENISA top 15 fenyegetésének listáján melyik támadás célpontja lehet cég?

Válasszon ki egyet vagy többet:

- ☒ Webes támadás ✓
- ☒ Belső elkövető ✓
- ☒ Adatszivárogtatás ✓
- ☐ Személyiség lopás

Válasza helyes.

A helyes válaszok:

Webes támadás,

Belső elkövető,

Adatszivárogtatás

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

2018 és 2020 között a sikeres adathalász támadások száma növekedett, holott a támadás-kampányok száma csökkent. Azaz kevesebb kampány mellett több felhasználó esett áldozatul. Ez arra utal, hogy:

Válasszon ki egyet:

- ☐ A felhasználók tudatosabbak lettek.
- ☒ A felhasználók tudatossága csökkent. ✓
- ☐ A támadások célzottan elkerülték a tudatos felhasználókat.
- ☐ A támadók előzetesen vizsgálták a felhasználók biztonság tudatosságát.

Válasza helyes.

A helyes válasz:

A felhasználók tudatossága csökkent..

41 kérdés

Helyes

1,00/1,00 pont

A ZTA alapvetése, hogy:

Válasszon ki egyet vagy többet:

- ☒ a vállalati erőforrás- és adatbiztonság teljes körű megközelítése, amely magában foglalja az identitást (személyes és nem személyi entitások), a hitelesítő adatokat, a hozzáférés-kezelést, a műveleteket, a végpontokat, a tárhely-környezeteket és az összekapcsoló infrastruktúrát. ✓
- ☒ egy kiberbiztonsági paradigma, amely az erőforrások védelmére összpontosít, és arra az előfeltevésre, hogy a bizalmat soha nem adják meg implicit módon, hanem folyamatosan értékelni kell. ✓
- ☒ az erőforrásokat azokra korlátozzák, akiknek csak a küldetés végrehajtásához szükséges minimális jogosultságokat (például olvasási, írási, törlési) kell hozzáférniük és megadniuk ✓
- ☐ az adatbiztonság érdekében senki nem ismerheti meg az információt.

Válasza helyes.

A helyes válaszok:

a vállalati erőforrás- és adatbiztonság teljes körű megközelítése, amely magában foglalja az identitást (személyes és nem személyi entitások), a hitelesítő adatokat, a hozzáférés-kezelést, a műveleteket, a végpontokat, a tárhely-környezeteket és az összekapcsoló infrastruktúrát.,

egy kiberbiztonsági paradigma, amely az erőforrások védelmére összpontosít, és arra az előfeltevésre, hogy a bizalmat soha nem adják meg implicit módon, hanem folyamatosan értékelni kell.,

az erőforrásokat azokra korlátozzák, akiknek csak a küldetés végrehajtásához szükséges minimális jogosultságokat (például olvasási, írási, törlési) kell hozzáférniük és megadniuk

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

A ZTA alaptétele, hogy:

Válasszon ki egyet vagy többet:

- ☒ Minden adatforrás és számítástechnikai szolgáltatás erőforrásnak minősül. ✓
- ☒ Az erőforrásokhoz való hozzáférést dinamikus házirend határozza meg ✓
- ☒ Minden erőforrás-hitelesítés és engedélyezés dinamikus, és a hozzáférés engedélyezése előtt szigorúan betartandó ✓
- ☐ Egy vállalat több belső hálózatot, saját helyi infrastruktúrával rendelkező távoli irodát, távoli és/vagy mobil egyéneket, valamint felhőszolgáltatásokat üzemeltethet

Válasza helyes.

A helyes válaszok:

Minden adatforrás és számítástechnikai szolgáltatás erőforrásnak minősül. ,

Az erőforrásokhoz való hozzáférést dinamikus házirend határozza meg ,

Minden erőforrás-hitelesítés és engedélyezés dinamikus, és a hozzáférés engedélyezése előtt szigorúan betartandó

43 kérdés

Helyes

1,00/1,00 pont

A ZTA alaptétele, hogy:

Válasszon ki egyet vagy többet:

- ☒ A hálózat helyétől függetlenül minden kommunikáció biztonságos. A hálózati hely önmagában nem jelent bizalmat ✓
- ☒ A vállalat felügyeli és méri az összes tulajdonában lévő és kapcsolódó eszköz integritását és biztonsági helyzetét. ✓
- ☒ A vállalkozás a lehető legtöbb információt összegyűjti az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és ezt felhasználja biztonsági helyzetének javítására. ✓
- ☐ A legtöbb vállalati infrastruktúra hibrid zéró bizalom/perem alapú üzemmódban fog működni, miközben továbbra is befektet az IT-korszerűsítési kezdeményezésekbe és javítja a szervezeti üzleti folyamatokat

Válasza helyes.

A helyes válaszok:

A hálózat helyétől függetlenül minden kommunikáció biztonságos. A hálózati hely önmagában nem jelent bizalmat,

A vállalat felügyeli és méri az összes tulajdonában lévő és kapcsolódó eszköz integritását és biztonsági helyzetét. ,

A vállalkozás a lehető legtöbb információt összegyűjti az eszközök aktuális állapotáról, a hálózati infrastruktúráról és a kommunikációról, és ezt felhasználja biztonsági helyzetének javítására.

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

A ZTA három fő logikai komponenst tartalmaz:

Válasszon ki egyet vagy többet:

- ☒ Házirend motor (PE) ✓
- ☒ Házirend-adminisztrátor (PA) ✓
- ☒ Irányelv-végrehajtási pont (PEP) ✓
- ☐ Perimeter védelmi megoldás (FW)

Válasza helyes.

A helyes válaszok:

Házirend motor (PE),

Házirend-adminisztrátor (PA),

Irányelv-végrehajtási pont (PEP)

45 kérdés

Helyes

1,00/1,00 pont

A ZTA kiegészítésére az alábbiak alkalmazhatók:

Válasszon ki egyet vagy többet:

- ☒ Fenygetés-információs hírfolyam(ok) ✓
- ☒ Hálózati és rendszertevékenységi naplók ✓
- ☒ Folyamatos diagnosztikai és kockázatcsökkentő (CDM) rendszer ✓
- ☒ Vállalati nyilvános kulcsú infrastruktúra (PKI) ✓

Válasza helyes.

A helyes válaszok:

Fenygetés-információs hírfolyam(ok),

Hálózati és rendszertevékenységi naplók,

Folyamatos diagnosztikai és kockázatcsökkentő (CDM) rendszer,

Vállalati nyilvános kulcsú infrastruktúra (PKI)

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Milyen biztonsági problémák vannak egy ilyen típusú használattal?

http://user:pass@example.tld:8080

Válasszon ki egyet:

- ☐ Az URL teljesen rendben van, séma szerinti.
- ☒ A http titkosítatlan, tehát a felhasználói név és jelszó olvasható. ✓
- ☐ A 8080-as port nem szokványos port webes kommunikáció esetén.
- ☐ Az example.tld nem engedélyezett

Válasza helyes.

A helyes válasz:

A http titkosítatlan, tehát a felhasználói név és jelszó olvasható..

47 kérdés

Helyes

1,00/1,00 pont

A HTTPS legfontosabb biztonsági előnyei:

Válasszon ki egyet vagy többet:

- ☒ Felek azonosítása külső tanúsító szervezetek (Certificate Authorities, CA) segítségével ✓
- ☒ Lehetőséget biztosít hibásan azonosított weboldalak automatikus tiltására – feltételezhető valamilyen rosszindulatú cselekmény ✓
- ☒ Adatok védelme erős titkosítás segítségével ✓
- ☐ Erős titkosítással tárolja a megadott adatokat.

Válasza helyes.

A helyes válaszok:

Felek azonosítása külső tanúsító szervezetek (Certificate Authorities, CA) segítségével,

Lehetőséget biztosít hibásan azonosított weboldalak automatikus tiltására – feltételezhető valamilyen rosszindulatú cselekmény,

Adatok védelme erős titkosítás segítségével

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Az alábbiak közül melyik támadás?

Válasszon ki egyet vagy többet:

- ☒ Trükkös kódolás (URL kódolás, homoglyph támadás) ✓
- ☒ Címhamisítás (DNS, DHCP, IP, ARP) ✓
- ☒ Közbeékelődés (MitM) ✓
- ☒ Lehallgatás (snifing, wiretapping) ✓

Válasza helyes.

A helyes válaszok:

Trükkös kódolás (URL kódolás, homoglyph támadás) ,

Címhamisítás (DNS, DHCP, IP, ARP) ,

Közbeékelődés (MitM) ,

Lehallgatás (snifing, wiretapping)

49 kérdés

Helyes

1,00/1,00 pont

Az alábbiak közül melyik támadás nem tartozik a Social Engineering támadások körébe?

Válasszon ki egyet:

- ☐ Phishing ("A fiókod lejárt, újítsd meg itt")
- ☐ Kattintásvadászat ("Sosem fogod kitalálni, hogy aztán mi történt...")
- ☐ Rémisztgetés ("A számítógéped fertőzött, kattints a segítségért")
- ☒ Szkriptelés (CSRF, XSS) ✓

Válasza helyes.

A helyes válasz:

Szkriptelés (CSRF, XSS).

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

0,00/1,00 pont

A weboldalak tartalmát hierarchiába lehet rendezni:

<https://neptun.uni-obuda.hu/hallgato/login.aspx>

Mit jelent az URL-ben a "/"?

Válasszon ki egyet:

- ☒ A könyvtárstruktúrát ✖
- ☐ A weboldalon egy hivatkozást
- ☐ Szakaszhatárt a weboldalon
- ☐ Beviteli mező értékét írja le.

Válasza helytelen.

A helyes válasz:

A weboldalon egy hivatkozást.

51 kérdés

Helyes

1,00/1,00 pont

Az SMTP protokoll:

Válasszon ki egyet vagy többet:

- ☒ A levelezőrendszerek közötti e-mail küldésre használt protokoll. ✔
- ☒ A 25-ös port van fenntartva a kommunikációra ✔
- ☐ Felhasználói üzenetmegjelenítésre szolgál.
- ☐ Titkosított kommunikációt biztosító protokoll.

Válasza helyes.

A helyes válaszok:

A levelezőrendszerek közötti e-mail küldésre használt protokoll.,

A 25-ös port van fenntartva a kommunikációra

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Az e-mail fejléce az alábbiakat tartalmazza:

Válasszon ki egyet vagy többet:

- ☒ Címzett (To) ✓
- ☒ Másolat (Cc) ✓
- ☐ Többcélú internetes levél kiterjesztés (sMIME)
- ☒ Dátum (Date) ✓

Válasza helyes.

A helyes válaszok:

Címzett (To),

Másolat (Cc),

Dátum (Date)

53 kérdés

Helyes

1,00/1,00 pont

Üzenettörzs tartalmi típusai:

Válasszon ki egyet vagy többet:

- ☒ multipart/mixed – több rész ✓
- ☒ text/plain – szöveges rész ✓
- ☒ text/html – formázott szöveges rész ✓
- ☒ application/octet-stream – mellékletek ✓

Válasza helyes.

A helyes válaszok:

multipart/mixed – több rész ,

text/plain – szöveges rész ,

text/html – formázott szöveges rész ,

application/octet-stream – mellékletek

[Weboldal](#)[Help](#)[Donate](#)

757 tárgy, 161 506 kérdés

1,00/1,00 pont

Üzenet hitelesítésére az alábbiak közül melyik alkalmazás terjedt el?

Válasszon ki egyet vagy többet:

- ☐ Az e-mail fejlécének és tartalmának titkosítása.
- ☒ Az e-mail tartalmi részének hashelése, PGP alkalmazásával. ✓
- ☒ Az e-mail tartalmi részének hashelése S/MIME megoldással. ✓
- ☐ A Sender Policy Framework (SPF) alkalmazásával.

Válasza helyes.

A helyes válaszok:

Az e-mail tartalmi részének hashelése, PGP alkalmazásával.,

Az e-mail tartalmi részének hashelése S/MIME megoldással.

55 kérdés

Helyes

1,00/1,00 pont

E-maileken keresztül az alábbi támadások lehetségesek:

Válasszon ki egyet vagy többet:

- ☒ Phishing ("Fiókja felfüggesztésre került, kattintson ide: URL") ✓
- ☒ Feladó hamisítás ✓
- ☒ Scam-ek, csaló üzenetek ✓
- ☐ Jelszavak rögzítése keyloggerrel

Válasza helyes.

A helyes válaszok:

Phishing ("Fiókja felfüggesztésre került, kattintson ide: URL"),

Feladó hamisítás,

Scam-ek, csaló üzenetek

◀ SOCIAL ENGINEERING

Ugrás...

PÓTZH ▶

Weboldal

Help

Donate



757 tárgy, 161 506 kérdés