ECDL VIZSGAPÉLDATÁR

IT biztonság

Syllabus 1.0

www.ecdl.hu

Kiadja a Neumann János Számítógép-tudományi Társaság

ECDL IT BIZTONSÁG

ÁLTALÁNOS TUDNIVALÓK

- Sikeres *IT Biztonság* modulvizsga esetén a vizsgázó nemzetközi ECDL modulzáró bizonyítványt kap.
- Regisztrálni és vizsgázni kizárólag az NJSZT által az IT Biztonság modulból vizsgáztatásra feljogosított *akkreditált vizsgaközpontoknál* lehet.
- A regisztráció díja mindenki számára egységesen 4000 Ft, a vizsgadíjat a vizsgaközpontok határozzák meg.

A VIZSGAFELADATOK

- Vizsgát Windows, Linux vagy MAC-OS környezetben lehet tenni, az adott platformon működő irodai alkalmazások segítségével
- A követelményrendszert a *Syllabus 1.0* tartalmazza. A Syllabus 1.0 megtekinthető a www.ecdl.hu oldalon is.
- A vizsgafeladatokat a nemzetközi ECDL Alapítvány által jóváhagyott hivatalos Question and Test Base (QTB) magyarul elkészített Feladatbázisából választják ki.
- Minden vizsga-feladatlap 32 részfeladatból áll, amiből 30 elméleti, 2 pedig gyakorlati részfeladat. Minden elméleti részfeladat és minden gyakorlati részfeladat 1-1 pontot ér.
  Összesen **32** pontot lehet elérni.
  Sikeres a vizsga, ha a vizsgázó legalább **24** pontot (75%) elér.

A VIZSGA

1. A vizsga időtartama 45 perc
2. A vizsgateremből a vizsgával kapcsolatos anyagok nem kerülhetnek ki, azokat a vizsga befejeztével a vizsgáztatónak át kell adni.
3. A vizsgán kizárólag a vizsgaközpont által meghatározott háttértárolóra szabad dolgozni.
4. A vizsgán semmiféle segédeszköz nem használható, az internetet csak a feladatok végrehajtásához szabad használni
5. A vizsga alatt a vizsgázók sem egymással, sem a vizsgáztatóval nem beszélhetnek
6. A vizsga alatt a vizsgázók felügyelet nélkül a termet nem hagyhatják el.
7. Szabálytalanság esetén a vizsgát fel kell függeszteni, a vizsgázót a vizsgázásból ki kell zárni.

A vizsgához tanfolyamot végezni nem kötelező.

1. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés, megismerés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára.

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) a vírusok gyorsabban eljutnak a felhasználóhoz, minthogy a vírusdefiníciós fájlok frissülnének
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
c) nagy kiterjedésű területen összekapcsolt számítógépek együttese

d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Alkalmazásfejlesztések esetén melyik szakaszban kell a biztonsági szempontokat figyelembe venni?

a) a biztonsági szempontok figyelembe vétele nem feltétlen szükséges, csak ha marad elég idő a fejlesztés során
b) a biztonsági szempontokat a tesztelésnél kell figyelembe venni
c) a biztonsági szempontokat az élesbe állás engedélyezésekor kell figyelembe venni
d) a biztonsági követelményeket a fejlesztés legkorábbi szakaszától érvényesíteni kell.

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) Arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Melyik a böngészők által a számítógépen tárolt információcsomag?

a) tűzfal
b) trójai program
c) rendszerszinten rejtőző kártékony kód
d) süti

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mire kell ügyelni, hogy megelőzzük egy zsarolóvírus elindulását?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) ne nyissunk meg ismeretlen levelekben található fájlok és csatolmányokat
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Szükséges-e okostelefonokon is végpontvédelmet használni?

a) nem, mert az okoseszközök felismerik maguktól a fenyegetettségeket
b) lehet, de nem kötelező, ha olyan telefont használunk, ami nagyon drága
c) nem, mert úgysem hagyom el, nagyon vigyázok rá.
d) Igen, mivel ezek az eszközök is számítógépek és ugyanúgy veszélyben vannak mint a többi számítógép.

2. Nyissa meg a vizsgaközpont által megadott mappában található ***biztonsag.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promocio.ppt*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

2. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatás előfordulását

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet??

a) 1995 Európai Adatvédelmi Irányelv
b) 2001 Információs Társadalom Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Mi a legnagyobb veszélye a titkosított jelszószéfeknek?

a) ha elfelejtem a mesterjelszót, akkor nem fogok hozzáférni az eltárolt jelszavaimhoz
b) nehéz megjegyezni hozzáférési jelszót
c) drágák és csak bizonyos környezetekben futnak
d) a vírusirtó szoftverek gyakran hamisan riasztanak rájuk.

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerülésére
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz

b) megengedi bárki csatlakozását egy magánhálózathoz
c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
d) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) htt

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízó műsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makró
d) makrózott titkosított szöveg

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása

d) adatok mentése

1.29. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***level.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***halozat.doc*** fájlról a ***marciusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

3. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifinomult támadásokat
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN

d) USB

1.15. Mi a jelszószéfek előnye?

a) az alkalmazások automatikusan ki tudják választani belőlük a megfelelő jelszót
b) a jelszavak sosem járnak le, nem kell cserélgetni őket
c) egy titkosított fájlban tárolhatjuk a jelszavainkat, nem kell megjegyeznünk őket, csak a fájlt védő mester jelszót
d) Ha véletlen letörlöm a titkosított fájlt, akkor senki nem fog a jelszavaimhoz hozzáférni – igaz én sem.

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?

a) adatok biztonsági mentése
b) fájlok tömörítése
c) személyes adatok védelme
d) információbúvárkodás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mikor használnak egyszer használatos jelszót?

a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben

c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

1.22. Melyik adat törölhető a böngésző által?

a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

1.23. Melyikkel korlátozható az interneten töltött időtartam?

a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

1.24. Melyik a közösségi oldalakon előforduló fenyegetés?

a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?

a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

1.26. Mi a digitális aláírás eszköze?

a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?

a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) hackelés

1.28. Mi tartalmazhat rosszindulatú programkódot?

a) levélcsatolmány
b) süti
c) tűzfal
d) digitális aláírás

1.29. Melyik nyújt védelmet az adatvesztés ellen?

a) sütik
b) kikérdezés
c) titkosított USB lemez használata
d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

2. Nyissa meg a vizsgaközpont által megadott mappában található ***hozzaferes.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***hozzaferes*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***rendszer.doc*** fájlról a ***juniusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

4. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik kiberbűnözés az alábbiak közül?

a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) adathalászat
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

1.3. Miért kell védeni az üzletileg érzékeny információkat?

a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) trójai program

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program

c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Mi eredményezhet jogosulatlan adathozzáférést??

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) jellemzően magánszemélyek weboldalai
c) on-line webáruház
d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 

b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok

b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését/megsemmisítését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található ***iroszer.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***ertekesites.xls*** fájlról a ***juliusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

5. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl 5*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tényező
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) tárhely takarékosság
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak

b) csak a pénzügyi intézmények számára fontosak

c) csak olvasni kell őket, de nem kell alkalmazni

d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok jogosulatlan felhasználók által hozzáférhetővé váltak

b) hamis név használata egy közösségi oldalon

c) a tűzfalat kikapcsolják

d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon

b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához

c) adatok elektromágneses eszközökkel történő megsemmisítése

d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés

b) rendszerszinten tevékenykedő kártékony kód

c) biometria

d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét

b) adatok elektromágneses eszközökkel történő megsemmisítését

c) alhálózatokat

d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését

b) nem lehetséges a vírus-ellenőrzést ütemezni

c) naprakészen kell tartani a vírusdefiníciós fájlokat

d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések

b) ezek törölve lettek a számítógépről

c) visszaállíthatók, ha szükséges

d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének??

a) internetről letöltött ideiglenes fájlok törlése

b) a program hibájának vagy biztonsági kockázatának kijavítása

c) sütik törlése

d) automatikus kiegészítés engedélyezése

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese

b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

c) nagy kiterjedésű területen összekapcsolt számítógépek együttese

d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból

b) biztosítani a mentéshez a biztonságos adattárolókat

c) védeni a hálózatot a betörésektől

d) automatikusan frissíteni a digitális tanúsítványokat

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
d) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni

b) a sütiket frissíteni kell

c) az adatokhoz hozzá akarnak férni mások is

d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett vezeték nélküli hálózat ikonja?

a) 

b) 

c) 

d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980

b) 12092010

c) jb

d) jenniferBloggs

1.20. Mi azonosítja a biztonságos weboldalakat?

a) .org

b) .com

c) https

d) http

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a forgalom felügyelete engedélyezési listákkal

b) a webforgalom átirányítása egy hamisított weboldalra

c) a kifigyelés egyik módszere

d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés

b) makrók tiltása

c) titkosítás

d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat

b) sütiket

c) digitális tanúsítványokat

d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver

b) kémszoftver

c) adathalász szoftver

d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést

b) becenevet

c) otthoni címet

d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl

b) digitális aláírás

c) makrózott titkosított szöveg

d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál

b) információkat kifigyelni valaki válla felett

c) félrevezetni valakit az interneten értékes információk megszerzéséért

d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz

b) levélcsatolmány megnyitása

c) elektronikus levél írása

d) adatok mentése

1.29. Mi lehet oka az azonnali üzenetek sebezhetőségének?

a) hátsó ajtó hozzáférés

b) valós idejű hozzáférés

c) vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat

b) áramellátás kiesése

c) tárcsázás

d) elektromágneses törlés

2. Nyissa meg a ***biztonsag*** fájlt a Vizsgakönyvtárból! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a Vizsgakönyvtárban található ***promocio*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

6. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
d) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett vezeték nélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***level.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***halozat.doc*** fájlról a ***marciusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

7. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) keresőmotor
c) on-line webáruház
d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 
b) 
c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok
b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Nyissa meg a vizsgaközpont által megadott mappában található ***hozzaferes.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***hozzaferes*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***rendszer.doc*** fájlról a ***juniusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

8. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

a) tűzfal
b) tartalomellenőrző szoftver
c) rosszindulatú programkód
d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz

b) megengedi bárki csatlakozását egy magánhálózathoz
c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mi a tűzfal korlátja?

a) fertőzött fájlokat helyez a karanténba
b) nem értesít automatikusan a hálózati behatoláskor
c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Alkalmazásfejlesztések esetén melyik szakaszban kell a biztonsági szempontokat figyelembe venni?

a) a biztonsági szempontok figyelembe vétele nem feltétlen szükséges, csak ha marad elég idő a fejlesztés során
b) a biztonsági szempontokat a tesztelésnél kell figyelembe venni
c) a biztonsági szempontokat az élesbe állás engedélyezésekor kell figyelembe venni
d) a biztonsági követelményeket a fejlesztés legkorábbi szakaszától érvényesíteni kell.

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) a web-oldal biztonságához
b) az automatikus kiterjesztés bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) személyazonosság lopás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Melyik a böngészők által a számítógépen tárolt információcsomag?

a) tűzfal
b) trójai program
c) rendszerszinten rejtőző kártékony kód
d) süti

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Keresse meg a vizsgaközpont által megadott mappában található ***iroszer.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***ertekesites.xls*** fájlról a ***juliusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

9. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

a) tűzfal
b) tartalomellenőrző szoftver
c) rosszindulatú programkód
d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz

b) megengedi bárki csatlakozását egy magánhálózathoz
c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mi a tűzfal korlátja?

a) fertőzött fájlokat helyez a karanténba
b) nem értesít automatikusan a hálózati behatoláskor
c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Alkalmazásfejlesztések esetén melyik szakaszban kell a biztonsági szempontokat figyelembe venni?

a) a biztonsági szempontok figyelembe vétele nem feltétlen szükséges, csak ha marad elég idő a fejlesztés során
b) a biztonsági szempontokat a tesztelésnél kell figyelembe venni
c) a biztonsági szempontokat az élesbe állás engedélyezésekor kell figyelembe venni
d) a biztonsági követelményeket a fejlesztés legkorábbi szakaszától érvényesíteni kell.

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mikor használnak egyszer használatos jelszót?

a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben
c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

1.22. Melyik adat törölhető a böngésző által?

a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

1.23. Melyikkel korlátozható az interneten töltött időtartam?

a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

1.24. Melyik a közösségi oldalakon előforduló fenyegetés?

a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?

a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

1.26. Mi a digitális aláírás eszköze?

a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?

a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) zsarolóvírus

1.28. Mi tartalmazhat rosszindulatú programkódot?

a) levélcsatolmány
b) süti

c) tűzfal
d) digitális aláírás

1.29. Melyik nyújt védelmet az adatvesztés ellen?

a) sütik
b) kikérdezés
c) titkosított USB lemez használata
d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

2. Nyissa meg a vizsgaközpont által megadott mappában található ***biztonsag.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promocio.ppt*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

10. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Mi a legnagyobb veszélye a titkosított jelszószéfeknek?

a) ha elfelejtem a mesterjelszót, akkor nem fogok hozzáférni az eltárolt jelszavaimhoz
b) nehéz megjegyezni hozzáférési jelszót
c) drágák és csak bizonyos környezetekben futnak
d) a vírusirtó szoftverek gyakran hamisan riasztanak rájuk.

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz
b) megengedi bárki csatlakozását egy magánhálózathoz
c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) jellemzően magánszemélyek honlapjai
c) on-line webáruház

d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 

b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl

c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok
b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található ***level.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***halozat.doc*** fájlról a ***marciusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

11. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a válaszfájl nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifigyelést
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzés mentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 

b) 

c) 

d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

a) nem lehet hozzáférni a privát hálózathoz
b) megfertőződhet a számítógép rosszindulatú szoftverekkel
c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) a web-oldal biztonságához
b) az automatikus kiterjesztés bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?

a) tűzfal
b) trójai program
c) rendszerszinten rejtőző kártékony kód
d) süti

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található ***hozzaferes.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***hozzaferes*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***rendszer.doc*** fájlról a ***juniusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

12. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógép-használat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifigyelést
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
d) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra

c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior
d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***iroszer.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***ertekesites.xls*** fájlról a ***juliusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

13. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógép-használat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifigyelést
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található jellemzően http előtag a https helyett?

a) on-line bank
b) felhasználók saját weboldalai
c) on-line webáruház
d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 
b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok
b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok

d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Nyissa meg a vizsgaközpont által megadott mappában található ***biztonsag.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promocio.ppt*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

14. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

   1.1. Melyik kiberbűnözés az alábbiak közül?

   a) okostelefon ellopása
   b) internetes számla on-line befizetése
   c) bankkártya adatok ellopása on-line
   d) internetes rádióhallgatása on-line

   1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

   a) dDOS támadás
   b) etikus hackelés
   c) bankkártya adatainak lemásolása
   d) kikérdezés

   1.3. Miért kell védeni az üzletileg érzékeny információkat?

   a) mert megakadályozza az adatlopást
   b) ütemezett mentések lefutásának biztosítása miatt
   c) kéretlen üzenetek blokkolása miatt
   d) a biztonságos weboldalak azonosításáért

   1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

   a) bonyolult fájlnevek
   b) billentyűzet-leütés naplózása
   c) eltérítéses adathalászat
   d) titkosítás

   1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

   a) bizalmasság
   b) sértetlenség
   c) rendelkezésre állás
   d) hitelesség

   1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet??

   a) 1995 Európai Adatvédelmi Irányelv
   b) 2001 Információs Társadalom Irányelv
   c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
   d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program

c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezetéknélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Alkalmazásfejlesztések esetén melyik szakaszban kell a biztonsági szempontokat figyelembe venni?

a) a biztonsági szempontok figyelembe vétele nem feltétlen szükséges, csak ha marad elég idő a fejlesztés során
b) a biztonsági szempontokat a tesztelésnél kell figyelembe venni
c) a biztonsági szempontokat az élesbe állás engedélyezésekor kell figyelembe venni
d) a biztonsági követelményeket a fejlesztés legkorábbi szakaszától érvényesíteni kell

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mikor használnak egyszer használatos jelszót?

a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben
c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

1.22. Melyik adat törölhető a böngésző által?

a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

1.23. Melyikkel korlátozható az interneten töltött időtartam?

a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

1.24. Melyik a közösségi oldalakon előforduló fenyegetés?

a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?

a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

1.26. Mi a digitális aláírás eszköze?

a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?

a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) hackelés

1.28. Mi tartalmazhat rosszindulatú programkódot?

a) levélcsatolmány
b) süti

c) tűzfal
d) digitális aláírás

1.29. Melyik nyújt védelmet az adatvesztés ellen?

a) sütik
b) kikérdezés
c) titkosított USB lemez használata
d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

2. Nyissa meg a vizsgaközpont által megadott mappában található ***secure.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***secure*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promotion.ppt*** fájlról az ***april backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

15. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

   1.1. Melyik kiberbűnözés az alábbiak közül?

   a) okostelefon ellopása
   b) internetes számla on-line befizetése
   c) bankkártya adatok ellopása on-line
   d) internetes rádióhallgatása on-line

   1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

   a) dDOS támadás
   b) etikus hackelés
   c) bankkártya adatainak lemásolása
   d) kikérdezés

   1.3. Miért kell védeni az üzletileg érzékeny információkat?

   a) mert megakadályozza az adatlopást
   b) ütemezett mentések lefutásának biztosítása miatt
   c) kéretlen üzenetek blokkolása miatt
   d) a biztonságos weboldalak azonosításáért

   1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

   a) bonyolult fájlnevek
   b) billentyűzet-leütés naplózása
   c) eltérítéses adathalászat
   d) titkosítás

   1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

   a) bizalmasság
   b) sértetlenség
   c) rendelkezésre állás
   d) hitelesség

   1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

   a) 1997 Európai Adatvédelmi Szabályozás
   b) 2001 Európai Információs Társadalmi Irányelv
   c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
   d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program

c) zombi-hálózati szoftver
d) tűzfalak

1.15. Mi biztosítja a vezeték nélküli biztonságot?

a) WAN
b) LAN
c) Média Hozzáférési Kontroll (MAC)
d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
d) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett vezetéknélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra

c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior
d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalász
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***letter.doc***! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***network.doc*** fájlról a ***march*** backup könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

16. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik kiberbűnözés az alábbiak közül?

a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) dDOS támadás
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

1.3. Miért kell védeni az üzletileg érzékeny információkat?

a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet, hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program

c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) Arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Szükséges-e okostelefonokon is végpontvédelmet használni?

a) nem, mert az okoseszközök felismerik maguktól a fenyegetettségeket
b) lehet, de nem kötelező, ha olyan telefont használunk, ami nagyon drága
c) nem, mert úgysem hagyom el, nagyon vigyázok rá.
d) Igen, mivel ezek az eszközök is számítógépek és ugyanúgy veszélyben vannak mint a többi számítógép.

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat

d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található ***access.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be az ***access*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***system.doc*** fájlról a ***june backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

17. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese

b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

a) nem lehet hozzáférni a privát hálózathoz
b) megfertőződhet a számítógép rosszindulatú szoftverekkel
c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) Arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 

b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok
b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található ***pencils.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***sales.xls*** fájlról a ***july backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

18. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Mire kell ügyelni, hogy megelőzzük egy zsarolóvírus elindulását?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) ne nyissunk meg ismeretlen levelekben található fájlok és csatolmányokat
d) titkosítás használata

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai

b) tartalom-ellenőrző program
c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található jellemzően http előtag a https helyett?

a) on-line bank
b) felhasználók saját weboldalai
c) on-line webáruház
d) biztonságos weboldal

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található ***secure.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***secure*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promotion.ppt*** fájlról az ***april backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

19. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Mi a legnagyobb veszélye a titkosított jelszószéfeknek?

a) ha elfelejtem a mesterjelszót, akkor nem fogok hozzáférni a jelszavaimhoz
b) nehéz megjegyezni hozzáférési jelszót
c) drágák és csak bizonyos környezetekben futnak
d) a vírusirtó szoftverek gyakran hamisan riasztanak rájuk.

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) Arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 

b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok

b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található ***letter.doc***! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***network.doc*** fájlról a ***march*** backup könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

20. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógép-használat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz
b) megengedi bárki csatlakozását egy magánhálózathoz

c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

a) mert ha nem frissítünk elveszik a garancia
b) mert így gyorsabban fog menni a letöltés
c) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
a) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett vezetéknélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat

d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található ***access.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be az ***access*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***system.doc*** fájlról a ***june backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

21. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik kiberbűnözés az alábbiak közül?

a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) dDOS támadás
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

1.3. Miért kell védeni az üzletileg érzékeny információkat?

a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Mikor használnak egyszer használatos jelszót?

a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben
c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

1.22. Melyik adat törölhető a böngésző által?

a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

1.23. Melyikkel korlátozható az interneten töltött időtartam?

a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

1.24. Melyik a közösségi oldalakon előforduló fenyegetés?

a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?

a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

1.26. Mi a digitális aláírás eszköze?

a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?

a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) crackelés

1.28. Mi tartalmazhat rosszindulatú programkódot?

a) levélcsatolmány
b) süti

c) tűzfal
d) digitális aláírás

1.29. Melyik nyújt védelmet az adatvesztés ellen?

a) sütik
b) kikérdezés
c) titkosított USB lemez használata
d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

2. Keresse meg a vizsgaközpont által megadott mappában található ***pencils.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***sales.xls*** fájlról a ***july backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

22. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik kiberbűnözés az alábbiak közül?

a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) dDOS támadás
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

1.3. Miért kell védeni az üzletileg érzékeny információkat?

a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifinomult támadásokat
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Mire kell ügyelni, hogy megelőzzük egy zsarolóvírus elindulását?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) ne nyissunk meg ismeretlen levelekben található fájlokat és csatolmányokat
d) titkosítás használata

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Szükséges-e okostelefonokon is végpontvédelmet használni?

a) nem, mert az okoseszközök felismerik maguktól a fenyegetettségeket
b) lehet, de nem kötelező, ha olyan telefont használunk, ami nagyon drága
c) nem, mert úgysem hagyom el, nagyon vigyázok rá.

d) Igen, mivel ezek az eszközök is számítógépek és ugyanúgy veszélyben vannak mint a többi számítógép.

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található ***secure.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***secure*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promotion.ppt*** fájlról az ***april backup*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

23. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára.

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz
b) megengedi bárki csatlakozását egy magánhálózathoz
c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el.

1.16. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***iroszer.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***ertekesites.xls*** fájlról a ***juliusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

24. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi a “jelszó feltörés” jelentése?

a) személyes adatokat lopni on-line módon
b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
c) nem megfelelő jelszavak egymás utáni bevitele
d) a jelszó nyílt szöveges verziójának megszerzése

1.2. Mi jelent fenyegetést az adatokra?

a) titkosítás
b) emberi tevékenység
c) biometria
d) sütik

1.3. Mi az üzletileg érzékeny információk védelmének célja?

a) biztosítani a makrók engedélyezését
b) megakadályozni a vírusok terjedését
c) megelőzni az ügyfelek adataival való visszaélést
d) megakadályozni az internetes zaklatást

1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?

a) a fájlok tömörítése
b) internet-szűrő alkalmazása
c) adatmentés készítése
d) jelszóhasználat

1.5. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.6. Melyik a személyazonosság-lopás leírása?

a) felhasználói név használata az interneten
b) felvenni más személy azonosságát haszonszerzés céljából
c) munkahelyi adatok megadása internetes vásárláskor
d) tartalomellenőrző szoftverek használata internetezés közben

1.7. Mi a makrók tiltásának hatása?

a) a makró nem fog futni
b) a makró törölve lesz a fájlból
c) a makró még mindig helyesen fog futni
d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

a) nem lehet törölni
b) gyorsabban lehet menteni
c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

a) tűzfal
b) tartalomellenőrző szoftver
c) rosszindulatú programkód
d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

a) a makrók letiltása az alkalmazásokban
b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
c) a “vis maior” esetekre való hivatkozás
d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifinomult támadásokat
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN

c) WAN
d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Mi a legnagyobb veszélye a titkosított jelszószéfeknek?

a) ha elfelejtem a mesterjelszót, akkor nem fogok hozzáférni a letárolt jelszavaimhoz
b) nehéz megjegyezni hozzáférési jelszót
c) drágák és csak bizonyos környezetekben futnak
d) a vírusirtó szoftverek gyakran hamisan riasztanak rájuk.

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Melyik jelöli a biztonságos weboldalakat?

a) 

b) 

c) 

d) 

1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

a) vírusdefiníciós fájlok
b) titkosított adatbázis-mentési fájlok
c) makrók
d) digitális tanúsítványok

1.23. Miért kell a sütiket blokkolni a böngészőkben?

a) hogy vírusirtó szoftvert lehessen telepíteni
b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
c) hogy böngészhessünk ismeretlen weblapokon
d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

a) a személyes adatokhoz csak a barátok férhetnének hozzá
b) a személyes adatokat bárki megnézheti
c) a barátok barátai láthatnák a személyes adatokat
d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

a) X509v3 digitális tanúsítványok
b) tűzfalak
c) digitális aláírások
d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

a) rendszerszinten tevékenykedő kártékony kódok
b) tárcsázó programok
c) adathalászat
d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

a) rosszindulatú programkódokat tartalmazhat
b) lehet, hogy nagyon nagy a fájl
c) lehet, hogy titkosító kulcs szükséges a megnyitásához
d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

a) vírusdefiníciós fájlok

b) on-line emelt díjas tárcsázó programok
c) digitális tanúsítványok
d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

a) bankkártya lemásolás
b) ütemezés
c) kikérdezés
d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

a) az adatok átmozgatása a Lomtárba
b) a háttértároló elektromágneses törlése
c) a szoftveres adatmegsemmisítő eszközök használata
d) a DVD-k bedarálása

2. Nyissa meg a vizsgaközpont által megadott mappában található ***hozzaferes.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***hozzaferes*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***rendszer.doc*** fájlról a ***juniusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

25. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

a) adatfeldolgozás kimenete
b) logikai állítások kombinációja
c) nyers és nem szervezett tények összessége
d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógép-használat közben?

a) etikus hackelés
b) elektromágneses megsemmisítés
c) kiberbűnözés
d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

a) emberi tevékenység
b) zombi-hálózati szoftverek
c) rosszindulatú programkódok
d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

a) csalások megelőzése
b) sütik karbantartása
c) hátsó ajtó biztosítása
d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

a) rendelkezésre állás
b) sértetlenség
c) bizalmasság
d) hozzáférhetőség

1.6. Mi a szélhámosság (social engineering) közvetlen következménye?

a) jogosulatlan hozzáférés a számítógéphez
b) tárhely-problémákhoz vezet
c) alkalmazza a sütik blokkolási beállításait
d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

b) jelszó-visszaállítási eljárások összessége
c) üzenetküldés azonnali üzenetküldővel
d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

a) a fájl tulajdonosa könnyen azonosítható
b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
d) a kititkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
b) engedély nélkül használt szoftverek
c) tűzfal-beállítások ellenőrzésére használatos szoftver
d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

a) kémszoftver
b) zombi-hálózat szoftvere
c) tárcsázók
d) eltérítéses adathalászat

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program

c) zombi-hálózati szoftver
d) tűzfalak

1.15. Szükséges-e okostelefonokon is végpontvédelmet használni?

a) nem, mert az okoseszközök felismerik maguktól a fenyegetettségeket
b) lehet, de nem kötelező, ha olyan telefont használunk, ami nagyon drága
c) nem, mert úgysem hagyom el, nagyon vigyázok rá.
d) Igen, mivel ezek az eszközök is számítógépek és ugyanúgy veszélyben vannak mint a többi számítógép.

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) magánszemélyek saját weboldalai
c) on-line webáruház
d) biztonságos weboldal

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Alkalmazásfejlesztések esetén melyik szakaszban kell a biztonsági szempontokat figyelembe venni?

a) a biztonsági szempontok figyelembe vétele nem feltétlen szükséges, csak ha marad elég idő a fejlesztés során
b) a biztonsági szempontokat a tesztelésnél kell figyelembe venni
c) a biztonsági szempontokat az élesbe állás engedélyezésekor kell figyelembe venni
d) a biztonsági követelményeket a fejlesztés legkorábbi szakaszától érvényesíteni kell

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás

c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Keresse meg a vizsgaközpont által megadott mappában található ***level.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***halozat.doc*** fájlról a ***marciusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

26. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

   1.1. Melyik kiberbűnözés az alábbiak közül?

   a) okostelefon ellopása
   b) internetes számla on-line befizetése
   c) bankkártya adatok ellopása on-line
   d) internetes rádióhallgatása on-line

   1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

   a) dDOS támadás
   b) etikus hackelés
   c) bankkártya adatainak lemásolása
   d) kikérdezés

   1.3. Miért kell védeni az üzletileg érzékeny információkat?

   a) mert megakadályozza az adatlopást
   b) ütemezett mentések lefutásának biztosítása miatt
   c) kéretlen üzenetek blokkolása miatt
   d) a biztonságos weboldalak azonosításáért

   1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

   a) bonyolult fájlnevek
   b) billentyűzet-leütés naplózása
   c) eltérítéses adathalászat
   d) titkosítás

   1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

   a) bizalmasság
   b) sértetlenség
   c) rendelkezésre állás
   d) hitelesség

   1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

   a) 1997 Európai Adatvédelmi Szabályozás
   b) 2001 Európai Információs Társadalmi Irányelv
   c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
   d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

a) vírus-ellenőrzés közben figyelni kell a működését
b) nem lehetséges a vírus-ellenőrzést ütemezni
c) naprakészen kell tartani a vírusdefiníciós fájlokat
d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

a) szoftverfrissítések
b) ezek törölve lettek a számítógépről
c) visszaállíthatók, ha szükséges
d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
c) töröljük a sütiket
d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

a) kis földrajzi területen több összekötött számítógép együttese
b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

a) törölni a sütiket a számítógépről vagy a hálózatból
b) a mentéshez biztosítson biztonságos háttér-adattárolókat
c) védje a hálózatot a betörésektől
d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

a) nem lehet hozzáférni a privát hálózathoz
b) megfertőződhet a számítógép rosszindulatú szoftverekkel
c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a vezetéknélküli hálózatok hozzáféréséhez?

a) megelőzi a hálózathoz való csatlakozási késedelmet
b) biztosítja a vírusirtó szoftver naprakészségét
c) így csak jogos felhasználó használhatja a hálózatot
d) megvédi a hálózati tűzfalat

1.19. Melyik biometriai védelem?

a) adatok mentése
b) bankkártya lemásolása
c) kikérdezés
d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

a) Arra, hogy a böngésző és a weboldal közötti titkosított kapcsolat legyen a tranzakció ideje alatt
b) az automatikus kiterjesztések és beépülő modulok bekapcsolásához
c) a Lomtárnak a tranzakciót követő kiürítéséhez
d) a tranzakciót követő elektromágneses törléshez

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra

c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior
d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található ***biztonsag.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promocio.ppt*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

27. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi az előnye a vírusirtóknak?

a) megakadályozzák a kifinomult támadásokat
b) frissítik a digitális tanúsítványokat
c) felismerik a vírusokat a számítógépen
d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

a) nem lehet letölteni
b) nem lehet fertőzésmentesíteni
c) nem lehet törölni
d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

a) frissíti az ideiglenesen letöltött és tárolt fájlokat
b) frissíti a sütiket
c) lehetővé teszi az új fenyegetések elleni védelmet
d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

a) LAN
b) VPN
c) WAN
d) USB

1.15. Mi a hálózati adminisztrátor feladata?

a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
d) fenntartani a munkatársak szükséges adathozzáférését a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

a) elektromágneses törlés
b) tűzfalak
c) adathalászat
d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

a) 
b) 
c) 
d) 

1.18. Mik a leggyakoribb szavak, amiket a rosszindulatú programokat terjesztő e-mailek „Tárgy/Subject” mezői tartalmaznak?

a) reklám, vedd meg, akció
b) invoice, document, order, mail delivery failure, bill
c) free shipping, best prise, best offer
d) árengedmény, mega akció, kiárusítás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

a) elindítja a vírusirtó szoftvert
b) megakadályozza a jogosulatlan adat-hozzáférést
c) biztosítja a sütik engedélyezését
d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

a) digitális tanúsítvány
b) süti
c) makró
d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található ***iroszer.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***safefile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***ertekesites.xls*** fájlról a ***juliusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

28. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program
c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) magánszemélyek személyes honlapjai
c) on-line webáruház
d) biztonságos weboldal

1.21. Mit jelent az eltérítéses adathalászat (pharming)?

a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra
c) a kifigyelés egyik módszere
d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?

a) automatikus kiegészítés
b) makrók tiltása
c) titkosítás
d) elektromagnetikus törlés

1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?

a) makrókat
b) sütiket
c) digitális tanúsítványokat
d) vírusdefiníciós fájlokat

1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?

a) reklámokat megjelenítő szoftver
b) kémszoftver
c) adathalász szoftver
d) tartalomellenőrző szoftver

1.25. Mit nem szabad közzétenni egy közösségi oldalon?

a) zenei érdeklődést
b) becenevet
c) otthoni címet
d) kedvenc televízóműsort

1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?

a) jelszavas tömörített fájl
b) digitális aláírás
c) makrózott titkosított szöveg
d) ideiglenesen letöltött és tárolt fájl

1.27. Mi az adathalászat?

a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
b) információkat kifigyelni valaki válla felett
c) félrevezetni valakit az interneten értékes információk megszerzéséért
d) az informatikai biztonsági hiányosságok tesztelése

1.28. Mi jelenti a legnagyobb kitettséget a rosszindulatú programkódoknak?

a) hozzáférés biztonságos weboldalhoz
b) levélcsatolmány megnyitása
c) elektronikus levél írása
d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

a) hátsó ajtó hozzáférés
b) valós idejű hozzáférés
c) vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

a) eltérítéses adathalászat
b) áramellátás kiesése
c) tárcsázás
d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található ***hozzaferes.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***hozzaferes*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***rendszer.doc*** fájlról a ***juniusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

29. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

a) bedarálás
b) adathalászat
c) etikus hackelés
d) titkosítás

1.2. Mit jelent a “hackelés” fogalma?

a) az adatokhoz való jogosulatlan hozzáférés megszerzése
b) félrevezetni a személyazonosságunkról valakit az interneten
c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

a) emberi tevékenység
b) adatlopás
c) tűz
d) vírusok

1.4. Mi a személyes adatok védelmének célja?

a) az etikus hackelés megelőzése
b) a személyazonosság-lopás megakadályozása
c) helyet lehessen megtakarítani a számítógép háttértárolóján
d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

a) csak az informatikusokra vonatkoznak
b) csak a pénzügyi intézmények számára fontosak
c) csak olvasni kell, de nem kell megvalósítani
d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak (social engineering)?

a) a személyes adatok mások által hozzáférhetővé váltak

b) hozzáférhetővé vált mások által a számítógép-rendszer
c) a tűzfalat kikapcsolják
d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

a) hamis név használata egy közösségi oldalon
b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
c) adatok elektromágneses eszközökkel történő megsemmisítése
d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

a) kikérdezés
b) rendszerszinten tevékenykedő kártékony kód
c) biometria
d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

a) zombi-hálózat szoftverét
b) adatok elektromágneses eszközökkel történő megsemmisítését
c) alhálózatokat
d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

a) a süti
b) a vírus
c) a digitális tanúsítvány
d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

a) biometria
b) vírus-definíciós fájl
c) süti
d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
c) minden adatot mentenek
d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

a) fájlok hozzáférés-védelmi beállításai
b) tartalom-ellenőrző program
c) zombi-hálózati szoftver
d) tűzfalak

1.15. Az alábbiak közül melyik egy már nem biztonságos vezeték nélküli hálózati forgalom titkosítási módszer?

a) WAN
b) LAN
c) WEP
d) WPA3

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

a) elektromágneses törlés
b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezetéknélküli hálózatot?

a) 
b) 
c) 
d) 

1.18. Hogyan történik a hálózati bejelentkezés?

a) felhasználói névvel és jelszóval
b) automatikus kiegészítéssel
c) titkosított felhasználói névvel
d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

a) használjon minél kevesebb karaktert a jelszóban
b) időnként változtassa meg a jelszavát
c) ossza meg a jelszavát a barátaival
d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

a) on-line bank
b) magánszemélyek saját weboldalai
c) on-line webáruház
d) biztonságos weboldal

1.21. Mikor használnak egyszer használatos jelszót?

a) a laptopra való első bejelentkezéskor
b) amikor a jelszót elküldik e-mailben
c) amikor tűzfalat állítanak be
d) VPN-be való bejelentkezéskor

1.22. Melyik adat törölhető a böngésző által?

a) kititkosított adat
b) titkosított adat
c) automatikus kiegészítés adata
d) billentyűzet-leütéseket naplózó adat

1.23. Melyikkel korlátozható az interneten töltött időtartam?

a) adathalász szoftver
b) szülői felügyelet szoftver
c) tárcsázó
d) sütik

1.24. Melyik a közösségi oldalakon előforduló fenyegetés?

a) bedarálás
b) elektromágneses törlés
c) bankkártya adatainak a lemásolása
d) szexuális kizsákmányolás

1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?

a) titkosítás
b) kikérdezés
c) eltérítéses adathalászat
d) kititkosítás

1.26. Mi a digitális aláírás eszköze?

a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
b) egy matematikai séma az üzenet hitelességének biztosítására
c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására

1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?

a) kifigyelés
b) internetes zaklatás
c) adathalászat
d) dDOS támadás

1.28. Mi tartalmazhat rosszindulatú programkódot?

a) levélcsatolmány
b) süti
c) tűzfal
d) digitális aláírás

1.29. Melyik nyújt védelmet az adatvesztés ellen?

a) sütik
b) kikérdezés

c) titkosított USB lemez használata
d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

a) az áramingadozásból adódó meghibásodások miatt
b) az adatok más általi visszaállíthatatlansága miatt
c) hogy tartalomellenőrző szoftvert lehessen telepíteni
d) hogy törölni lehessen minden sütit

2. Keresse meg a vizsgaközpont által megadott mappában található ***level.doc*** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a ***lockfile*** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***halozat.doc*** fájlról a ***marciusi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

30. FELADAT

Forrásfájlok helye: .....
Mentés helye és neve: .....

1. Nyissa meg a ***válaszfájl*** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik kiberbűnözés az alábbiak közül?

a) okostelefon ellopása
b) internetes számla on-line befizetése
c) bankkártya adatok ellopása on-line
d) internetes rádióhallgatása on-line

1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?

a) dDOS támadás
b) etikus hackelés
c) bankkártya adatainak lemásolása
d) kikérdezés

1.3. Miért kell védeni az üzletileg érzékeny információkat?

a) mert megakadályozza az adatlopást
b) ütemezett mentések lefutásának biztosítása miatt
c) kéretlen üzenetek blokkolása miatt
d) a biztonságos weboldalak azonosításáért

1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?

a) bonyolult fájlnevek
b) billentyűzet-leütés naplózása
c) eltérítéses adathalászat
d) titkosítás

1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?

a) bizalmasság
b) sértetlenség
c) rendelkezésre állás
d) hitelesség

1.6. Melyik a 2018. május 25-től kötelezően alkalmazandó személyes adatok védelméről szóló rendelet?

a) 1997 Európai Adatvédelmi Szabályozás
b) 2001 Európai Információs Társadalmi Irányelv
c) 2016/679 Általános Adatvédelmi Rendelet (GDPR – General Data Protection Regulation)
d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság (social engineering) módszerei közé?

a) közösségi oldalakhoz több fiókkal rendelkezni
b) valaki válla fölött megszerezni az információkat
c) videó- és hanghívásokat kezdeményezni az interneten
d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

a) a pénzügyi adatokat mások is használhatják
b) a vírusirtó nem működik a továbbiakban
c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítik és küldik károkozási célból?

a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
b) tűzfalak
c) rosszindulatú programkódok
d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

a) rendszerszinten tevékenykedő kártékony kódokat
b) elektromágneses elven alapuló adattörlési módszereket
c) tűzfalakat
d) bedarálást

1.11. Melyik egy fertőző rosszindulatú szoftver?

a) a féreg
b) a süti
c) a tűzfal
d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

a) a billentyűzetleütés naplózás a begépelt adatot rögzíti
b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

a) fertőzésmentesített fájlokat helyeznek a karanténba
b) észlelik a vírusokat, de nem törlik automatikusan őket
c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

a) nem kell jelszó a hálózati csatlakozáshoz
b) megengedi bárki csatlakozását egy magánhálózathoz

c) biztonságos saját hozzáférést biztosít a hálózathoz
d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mire kell ügyelnünk bankkártya használat esetén?

a) ne kopjon le a kártya hátuljára felírt PIN kód
b) ne adjuk ki a kártyát a kezünkből, vagy mindig legyen szem előtt, mert a kártyán lévő adatok ismeretében már lehet fizetni az interneten
c) ha fordítva ütjük be a PIN kódunkat, akkor az ATM hívja a TEK-et.
d) a kártya hátoldalán ne lógjon ki az aláírás minta, mert akkor már nem fogadják el

1.16. Miért kell a vezetéknélküli eszközökön firmware programot frissíteni?

d) mert ha nem frissítünk elveszik a garancia
e) mert így gyorsabban fog menni a letöltés
f) mert a régi firmware verziók sérülékenyek és ez miatt feltörhetővé válik az eszköz.
a) mert a letöltéskor további segédprogramokat kapunk ajándékba a gyártótól.

1.17. Mit kell figyelembe venni nem védett vezetéknélküli hálózat használatakor?

a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett vezetéknélküli hálózat ikonja?

a) 
b) 
c) 
d) 

1.19. Melyik számít jó jelszónak?

a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

a) .org
b) .com
c) https
d) http

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c) 

d) 

1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?

a) dDOS támadás
b) eltérítéses adathalászat
c) etikus hackelés
d) információ-szerzés

1.23. Melyik a böngészők által a számítógépen tárolt információcsomag?

a) tűzfal
b) trójai program
c) rendszerszinten rejtőző kártékony kód
d) süti

1.24. Mitől kell tartanunk a közösségi média használatakor?

a) biometria
b) etikus hackelés
c) internetes zaklatás
d) titkosított fájlok

1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?

a) az elektronikus levél aláírással való ellátása
b) az elektronikus levél titkosítása
c) egyszerű szöveges elektronikus levél formázása
d) definíciós fájl hozzáadása az elektronikus levélhez

1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?

a) adathalászat
b) kifigyelés
c) billentyűzet-leütés naplózás
d) zombi-hálózati szoftver

1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?

a) elektronikus levél
b) fájl-megosztás
c) eltérítéses adathalászat
d) azonnali üzenetküldés

1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?

a) a tűzfal bekapcsolása
b) a tűzfal kikapcsolása
c) a fájl-megosztás korlátozása
d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

a) vírusirtó szoftver
b) titkosított szöveges dokumentumok
c) biztonsági kábel
d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

a) az adatok Lomtárba mozgatása
b) az adatokat tartalmazó lemez bedarálása
c) jelszavas tömörítés alkalmazása
d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található ***biztonsag.doc*** fájlt! Tegye megnyitás-védetté a fájlt, a ***guardfile*** jelszó használatával! Mentse el és zárja be a ***biztonsag*** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található ***promocio.ppt*** fájlról az ***aprilisi_mentes*** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.