**Képzési adatlap**

|  |  |  |
| --- | --- | --- |
| **Cím** | | Kiberbiztonság otthon és az irodában |
| **Kulcsszavak (meta tag)** | | kiberbiztonság, biztonság, rosszindulatú programok, adathalászat, érzékeny adatok, biztonság |
| **Készítette** | | Internet Web Solutions |
| **Nyelv** | | magyar |
| **Képzési terület (X, ahol alkalmazható)** | | |
|  | Innováció és szervitizáció | |
| **X** | Digitális átalakulás | |
|  | Lokalizáció | |
|  | Fenntarthatóság | |
| **ESCO kompetenciák és készségek** | | |
| * Transzverzális készségek és kompetenciák   + Szociális és érzelmi készségek   + Kritikus gondolkodás   + Analitikus gondolkodás   + Problémamegoldás   + Önmenedzsment   + Üzletvezetés   + Alkalmazkodóképesség   + Rugalmasság   + Kreativitás   + Hálózatépítés   + Kezdeményezés   + Rugalmasság   + Nyitottság   + A komplexitás megértése   + Együttműködés   + Empátia   + Innováció   + Vezetés      * Képességek   + Technológiai készségek   + Termékmarketing   + Digitális marketing   + Digitális készségek   + Kommunikáció   + Együttműködés   + Érzelmi intelligencia      * Tudás   + Üzletvezetés   + Online tanulás és képzés   + Reklám   + Felhőalapú számítástechnika   + Big Data   + E-kereskedelem   + Mesterséges intelligencia   + Dolgok internete (IoT)   + Digitális írástudás   + Kiberbiztonság   + Adatbányászat és elemzés   + Fenntarthatóság   + Jólét   + Éghajlatváltozás   + Közösségi média menedzsment | | |
| **Ízelítő** | | |
| "Tudta, hogy az európai KKV-k 85%-a a kiberbiztonságot kulcsfontosságúnak tartja vállalkozása számára?" | | |
| **Célkitűzések / célok / tanulási eredmények** | | |
| A modul végén a következő ismereteket és képességeket sajátíthatja el:   * A kiberbiztonság fogalmának megértése és a főbb veszélyek. * A leggyakoribb kibertámadási kockázatok megértése és megelőzése otthoni és irodai munkavégzés esetén. * Biztonságos böngészés az interneten, mind munka közben, mind a mindennapi feladatok elvégzése során. * Az informatikai és kiberbiztonsági ismeretek fejlesztése. | | |
| **Leírás** | | |
| Az európai KKV-k többsége a kiberbiztonságot kulcsfontosságú üzleti kérdésnek tekinti. A járvány utáni időszakban azonban nem minden vállalat hajtott végre új biztonsági intézkedéseket a távmunkából eredő kockázatok leküzdésére, mivel a tudatosság és a kiberbiztonsági ismeretek hiánya miatt nem minden vállalat alkalmazza ezeket. Ez a modul lehetővé teszi a KKV-k alkalmazottai és vállalkozói számára, hogy fejlesszék kiberbiztonsági készségeiket és ismereteiket a digitális készségek és a kiberbiztonsággal szembeni ellenálló képességük növelése érdekében. | | |
| **Az előnyök ellenőrző listája vállalkozók számára** | | |
| ✓ A kiberbiztonsági stratégiák végrehajtása a KKV-kban csökkenti az információvesztés és -szivárgás kockázatát, miközben fenntartja az adatok integritását.  ✓ Az ügyféladatok bizalmas kezelésével a vállalkozás hírneve és vállalati imázsa is javul a nyilvánosság előtt.  ✓ A kiberbiztonság növeli a vállalatok ellenálló képességét és helyreállítási kapacitását, a biztonsági mentések lehetővé teszik számukra, hogy egy váratlan incidens után újraindítsák az üzletmenetet.  ✓ A kibertámadások vagy belső problémák miatti információveszteség csökkentésével a termelékenység is nő.  ✓ A kiberbiztonság alapvető eszköz a munkáltatók és a munkavállalók számára, nemcsak a munkában, hanem a magánéletben is, a tudatosság növelése és a kiberkockázatok megelőzése révén (pl. az online vásárlás során). | | |
| **Tartalom 3 szintre rendezve** | | |
| **Modul: Kiberbiztonság otthon és az irodában**  **1. egység: A kiberbiztonság alapjai**  **1.1. szakasz: Mi az a kiberbiztonság?**  A **„kiberbiztonság”** kifejezés az 1970-es években született, mivel a vállalatoknak meg kellett **védeniük számítógépes rendszereiket** a rosszindulatú támadásoktól, amelyek az információkkal való visszaélés révén veszélyeztethetik azok megfelelő működését.  A kiberbiztonság magába foglalja az eszközök, technológiák, irányelvek, szabályozások és eljárások használatát a hálózatok, rendszerek, eszközök és alkalmazások védelmére vagy helyreállítására a **kibertámadásokkal** szemben, amelyek célja az bizalmas információkhoz való hozzáférés, azok megsemmisítése vagy megváltoztatása, a munkafolyamatok megzavarása vagy a szervezetek vagy egyének pénzének kihasználása.  Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) 2021-es jelentése szerint a megkérdezett 249 európai kis- és középvállalkozások (KKV) **85%-a a kiberbiztonságot kulcsfontosságúnak tartja vállalkozása számára.** A világjárványt követő időszakban a KKV-k 45%-a vezetett be új technológiákat, azonban ezek 90%-a azonban nem tartalmazott új biztonsági intézkedéseket.  Ugyanez a jelentés, amely értékes információkkal szolgál az európai KKV-k kiberbiztonságáról, **az európai KKV-k által elszenvedett főbb kiberbiztonsági incidenseket mutatja be eredetük alapján,** ahogy az alábbi grafikonon látható.  Forrás: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (saját kimutatás)  **1.2. szakasz: Főbb fogalommeghatározások**  Általános biztonság:   * **Biztonsági mentés**: A fájlok és programok másolata, amelyet más eszközökön vagy más adathordozókon tárolnak annak érdekében, hogy meghibásodás, elvesztés vagy lopás esetén az információkat vissza lehessen állítani. * **Bizalmas adatok**: Magánjellegű vagy bizalmas információkat, például személyes vagy banki adatokat tartalmazó információk. * **Szoftver**: A szoftver olyan számítógépes program, amelyet meghatározott feladatok elvégzésére terveztek, például egy böngésző, egy játék stb. A „hardver" ellentéte, hiszen az az eszköz fizikai összetevőit, például az alaplapot vagy a processzort foglalja magába. * **Titkosítás**: A folyamat során egy dokumentum vagy fájl olyan információvá alakul át, amely olvashatatlan azok számára, akik nem rendelkeznek a dekódoláshoz szükséges kulccsal. Arra szolgál, hogy megvédje az információkat az illetéktelen személyekkel szemben. * **HTTP / HTTPS**: Az egyik legszélesebb körben használt protokoll az internetes böngészéshez. A HTTPS (HyperText Transfer Protocol Secure) a biztonságos változat. Ez a protokoll biztosítja, hogy az Ön eszköze és a weboldal között továbbított információk titkosítva és védve legyenek. * **Tűzfal:** Az interneten való böngészés és egy weboldal elérése során kommunikál a számítógéppel a kapcsolat létrehozása érdekében. A tűzfal elemzi az ilyen típusú kapcsolatokat, annak érdekében, hogy megakadályozhassa a hozzáférést azokhoz, amelyek kockázatot jelenthetnek.   Veszélyek:   * **Pszichológiai manipuláció**: A pszichológiai manipuláció nem igényel magas szintű számítógépes ismereteket, mivel az emberek pszichológiai technikák és szociális készségek segítségével történő manipulációját jelenti, és gyakran használják érzékeny információk, például jelszavak vagy banki adatok megszerzésére. Az adathalász technikák a társadalmi manipulációra épülnek. * **Adathalászat**: Az a technika, amikor e-mailben egy másik személynek vagy szervezetnek adják ki magukat, és a felhasználót arra késztetik, hogy valamilyen műveletet hajtson végre egy hamisított oldalon jelszavak megszerzése vagy egy fertőzött fájl letöltése érdekében. * **SMS adathalászat**: SMS és adathalászat. Az adathalászathoz hasonlóan ez a technika SMS-üzeneteket használ ugyanarra a célra. * **Hangalapú adathalászat**: Hang és adathalászat. Ebben az esetben a támadó egy telefonhívás során valaki másnak adja ki magát, gyakran a készülék vagy a telefontársaság műszaki segítségnyújtójának szerepét játszva. * **Webalapú támadások**: Ezek az összetett támadások akkor lépnek fel, amikor a felhasználó az interneten böngészik, és rosszindulatú szoftverek segítségével megfertőzik azokat az eszközöket, amelyek nem rendelkeznek a szükséges védelemmel vagy elavultak.   A rosszindulatú programok típusai:   * **Rosszindulatú szoftverek**: Ezek a rosszindulatú szoftverek különböző formákat ölthetnek (futtatható kódként, szkriptek formájában stb.), és olyan műveleteket végezhetnek, mint a bizalmas adatok titkosítása vagy törlése, az eszköz alapvető funkcióinak megváltoztatása, a felhasználói tevékenység utáni kémkedés, és így tovább. A rosszindulatú szoftverek elleni védelmet az olyan szoftverek (anti-malware) alkalmazása jelenti, amelyek képesek arra, hogy felismerjék, eltávolítsák ezekat a káros szoftvereket. A rosszindulatú szoftvereknek számos típusa létezik. Ezeket a következő diákon fogjunk megvizsgálni. * **Számítógépes vírus**: Az ilyen típusú rosszindulató szoftver célja az eszköz működésének megváltoztatása. A felhasználó közreműködését igényli a különböző fájlokra és rendszerekre való átterjedéshez. * **Számítógépes féreg**: Képes replikálódni és átkerülni egy fertőzött eszközről a hálózaton keresztül más eszközökre. Gyakran fertőzött USB-meghajtókról, e-mail mellékletekről vagy akár webhelyekről származik. * **Trójai vírus**: Az ilyen típusú rosszindulatú szoftverek ártalmatlan fájlként vagy szoftverként jutnak be a rendszerbe, és a háttérben nem kívánt műveleteket hajtanak végre, például fájlokat törölnek vagy más rosszindulatú szoftverek töltenek le. * **Kémszoftver**: Ahogy a neve is mutatja, ez a fajta rosszindulatú szoftver kémkedik a fertőzött eszközön, és információkat gyűjt a felhasználó tevékenységéről. Általában kéretlen elektronikus üzenetekből (spam) vagy hamis letöltő webhelyekről származik. * **Reklámszoftver**: Az a rosszindulatú szoftver, ami nyomon követi a felhasználó böngészőjét és letöltési előzményeit, hogy nem kívánt hirdetéseket jelenítsen meg a felhasználó számára, amelyekre rákattinthat. Általában fertőzött webhelyeken vagy hamis letöltési webhelyeken keresztül fertőzik meg az eszközöket. * **Zsarolószoftver**: A rosszindulatú szoftverek veszélyes típusa, amely titkosítja a fájlokat az eszköz merevlemezén, és korlátozza a felhasználó hozzáférését. A fájlok visszafejtéséért cserébe váltságdíjat követel, általában kriptovalutában. Jól ismert eset a WannaCry.   **2. egység: Kiberbiztonság...**  **2.1. szakasz: ...a munkahelyen**  **A kiberbiztonság a vállalaton belül mindenki felelőssége,** úgy a vezetőségnek, mint az alkalmazottaknak, ezért a vállalati munkakultúra részévé kell válnia.  Mind az irodában, mind az otthoni környezetben feltétlenül szükséges az **alapvető intézkedések betartás**a. A vállalkozás megfelelő működéséhez mindez **kiberbiztonsági terv keretén belül** valósul meg.  Az alábbiakban egy **alapvető kiberbiztonsági tervet** mutatunk be. Ezt a javaslatot ajánlott követni a vállalati információk sértetlenségének megőrzése érdekében:   1. **Tájékoztatás a vállalat kiberbiztonsági irányelveiről.** Minden vállalat egyedi igényekkel rendelkezik, ezért a kiberbiztonsági kultúra megteremtése érdekében a kiberbiztonsági irányelveket minden alkalmazottnak és vezetőnek ki kell dolgoznia és be kell tartania. 2. **Az eszközök szoftverének frissítése.** Az összes alkalmazás és operációs rendszer naprakészen tartása megelőzi a sebezhetőségüket. 3. **Tűzfal felállítása.** A tűzfal további védelmet nyújt az interneten való navigálás során. 4. **Rendszeres biztonsági mentések készítése.** Adatvesztés esetén a biztonsági mentések segítenek a gyors helyreállításban. 5. **A wifi hálózatok védelme.** A mindennapi tevékenységek során használt wifi-hálózatokat megfelelően kell konfigurálni, hogy kellően biztonságosak legyenek egy lehetséges harmadik féllel szemben. 6. **Olyan programokat telepítése, amelyek képesek elhárítani a rosszindulatú szoftvereket.** Ezek a szoftverek védelmet nyújtanak a támadásokkal szemben. 7. **Cselekvési terv kidolgozása a mobileszközök esetében**. A kiberbiztonság nemcsak a számítógépekre vonatkozik, hanem a mobil eszközökre, például az okostelefonokra és a táblagépekre is, amelyeket szintén védeni kell. 8. **Különböző eljárások bevezetése az információk védelme érdekében.** Ki kell alakítani a kiberbiztonsági incidensek esetén követendő eljárásokat, szükséges lépéseket. 9. **Erős jelszavak használata.** Ennek érdekében kombinálják a számokat, betűket és speciális karaktereket. A jelszavak biztonságosságának ellenőrzésének egyik módja a https://password.kaspersky.com/ weboldal. 10. **A szoftverek telepítéséhez szükséges jogosultságok korlátozása.** Az alkalmazottaknak korlátozott hozzáféréssel kell rendelkezniük az új szoftverek telepítésekor, hogy megakadályozzák a hálózati eszközöket megfertőző, csalárd alkalmazások telepítését.   **2.2. szakasz: ...a távmunkában**  Távmunka esetén a kiberbiztonság még fontosabb, mivel otthoni munkavégzés esetén nincs ugyanakkora ellenőrzés a vállalat kiberbiztonsági eljárásait és irányelveit illetően, a hálózatok kevésbé biztonságosak, előfordulhatnak konfigurációs hibák, hiányzik a képzés, stb.  Ezért új intézkedések bevezetését kell mérlegelni annak érdekében, hogy az információkhoz való távoli hozzáféréssel kapcsolatos alábbi kiberbiztonsági célkitűzések teljesülhessenek:   * **Hozzáférhetőség.** A felhatalmazott felhasználóknak szükség esetén hozzáféréssel kell rendelkezniük az információkhoz. * **Titoktartás.** Biztosítani kell, hogy csak az arra jogosult felhasználók férhessenek hozzá az információkhoz. * **Hitelesség.** Biztosítani kell, hogy azok a meghatalmazott felhasználók, akik hozzáférnek az információkhoz, valóban azok legyenek, akiknek vallják magukat. * **Nyomonkövethetőség.** Lehetővé kell tenni az információkhoz való illetéktelen vagy jogosulatlan hozzáférés nyomon követését. * **Integritás.** Biztosítani kell, hogy az információk és azok feldolgozási módszerei pontosak és teljeskörűek legyenek.   A fent említett kiberbiztonsági terv mellett erősen ajánlott a **VPN (virtuális magánhálózat)** használata. Ez a hálózati technológia biztonságos kapcsolatot tesz lehetővé a helyi hálózat és az internet között, így **az információk sértetlensége és bizalmas jellege garantált.**  Emellett a **távoli asztali hozzáférési alkalmazások** lehetővé teszik a távmunkások számára, hogy távolról irányítsák az irodában fizikailag található számítógépeket. Ilyen például a TeamViewer eszköz.  A **felhőmegoldások** és az **együttműködési eszközök** szintén fontos eszközei a távmunka kiberbiztonságának, mivel **lehetővé teszik az információkhoz való gyors és összehangolt hozzáférést.**  Néhány példa a távmunkában használt eszközökre:  **VPN:**   * **hide.me**. Ez a VPN szolgáltatás lehetővé teszi a privát böngészést, földrajzi korlátozások nélkül. Több mint 2000 szerverrel és 75 helyszínnel számol. <https://hide.me/> * **PrivadoVPN.** A svájci székhelyű, és ingyenes verziója havonta legfeljebb 10 GB adat védelmét teszi lehetőv. <https://privadovpn.com/>   **Távoli asztal:**   * **AnyDesk.** Olyan távoli asztali szoftver, amely szintén ingyenesen elérhető személyes használatra. Ez a fajta eszköz lehetővé teszi az információkhoz való hozzáférést bárhonnan, ami javítja a belső kommunikációt.. <https://anydesk.com/> * **TeamViewer.** Ez az eszköz inkább az információk távoli elérésére összpontosít, mivel biztosítja a hozzáférést bármely eszközhöz bárhonnan. Lehetővé teszi a biztonságos fájlmegosztást és a hozzáférést más eszközökhöz. Előnye, hogy személyes használatra ingyenes. <https://www.teamviewer.com/>   **Felhőalapú megoldások:**   * **Dropbox.** Az ingyenes csomag 2 GB tárhelyet biztosít, a fizetős csomagok pedig 3 TB tárhelyig kínálnak különböző megoldásokat. <https://www.dropbox.com/> * **MEGA.** Ez a platform 20 GB-ot tartalmaz ingyenesen, és magánszemélyek számára 16 TB-ig, vállalatok számára pedig 10 PB-ig terjedő fizetős csomagokkal rendelkezik, így ez az egyik legnagyobb kapacitású megoldás. <https://mega.io/>   **Együttműködési eszközök:**   * **Slack.** Ez az azonnali üzenetküldő platform lehetővé teszi az együttműködést más eszközökkel és egyszerűsíti a csapat kommunikációját. Az ingyenes verzió biztosítja a hozzáférést az utolsó 10.000 csapatüzenet előzményeihez, a kollégákkal folytatott videohívásokhoz, emellett 10 alkalmazással kompatibilis. <https://slack.com/> * **Trello.** Ez az eszköz a Kanban kártyarendszerrel működik, és lehetővé teszi, hogy jegyzeteket, fájlokat, határidőket és egyéb elemeket is felvegyen a rendszerbe. A kártyák rendezésével könnyen kezelhető, és több nyelven is elérhető. Ez az eszköz csapatonként legfeljebb 10 tábla erejéig ingyenes. <https://trello.com/>   **3. egység: Javaslatok vállalkozóknak és alkalmazottaknak**  **3.1. szakasz: Javaslatok vállalkozóknak**   * Győződjön meg róla, hogy cége rendelkezik olyan **kiberbiztonsági tervvel,** amely megfelel a vállalkozás igényeinek és potenciális sebezhetőségének. * Állítson fel irányelveket és eljárásokat a b**iztonságos információkezelésre**, például ne használjon személyes eszközöket, és a dokumentumokat biztonságosan semmisítése meg. * **Informálja, képezze alkalmazottait a kiberbiztonságról**, hogy be tudják tartani az irányelveket és eljárásokat. * **Fejlessze digitális és kiberbiztonsági készségeit**; ne feledje, hogy nagyon érzékeny információkat kezel. * Tartsa be az **alkalmazottakra vonatkozó javaslatokat** is!   **3.2. szakasz: Javaslatok alkalmazottaknak**   * A kiberbiztonság az információk **fizikai biztonságával kezdődik**: ne tároljon asztalán bizalmas információkat, a jelszavakat tartalmazó post-it-eket, e-maileket, stb. * Ne csatlakoztasson olyan **USB-eszközöket**, amelyek nem megbízható személyektől származnak, mivel megfertőzhetik a számítógépét. * **Az érzékeny információkat titkosítsa elküldés előtt**, például jelszóval védett tömörített fájlon keresztül. * Ne felejtse el rendszeresen **kiüríteni a számítógép lomtárát.** * Készítsen rendszeres **biztonsági mentéseket.** * A vállalaton kívül is **tartsa szemmel mobil eszközeit.** * Ha lehetséges, **kerülje a titkosítatlan wifihálózatokhoz való csatlakozást** a munkahelyi eszközökkel. Ha erre szükség van, használjon VPN-t a biztonság érdekében. * **Zárja le a számítógépét**, amikor távol van az íróasztalától. * **Használjon biztonságos jelszavakat**. Jelszavainak biztonságáról meggyőződhet a jelszavak ellenőrzésére szolgáló weboldalakon, például a<https://password.kaspersky.com/> oldalon. * **Ne használja mindig ugyanazokat a jelszavakat**, mert kiszivárgásuk esetén sebezhetőbbé válik. * **Ne töltsön le ismeretlen feladóktól csatolmányokat**, legyen óvatos a **gyanús üzenetekkel** szemben, és **minden incidenst jelentsen** a feletteseinek. | | |
| **Tartalom felsorolásban** | | |
| * A kiberbiztonság abból az igényből alakult ki, hogy a vállalatoknak meg kell védeniük számítógépes rendszereiket a rosszindulatú támadásoktól. * Az európai KKV-k által elszenvedett leggyakoribb kiberbiztonsági incidensek az adathalászattal kapcsolatosak. * A kiberbiztonság mindenki felelőssége egy vállalaton belül, és szükség van egy olyan kiberbiztonsági tervre, amelyet a vezetők, igazgatók és alkalmazottak megfelelően követnek. * A távmunkában a kiberbiztonságot olyan IKT-eszközök használata egészíti ki, amelyek lehetővé teszik a kiberbiztonság öt célkitűzésének teljesítését az információhoz való hozzáférés során. * A munkáltatónak gondoskodnia kell arról, hogy legyen kiberbiztonsági terv, és hogy a munkavállalók rendelkezzenek a terv betartásához szükséges készségekkel. * A munkavállalóknak elkötelezettnek kell lenniük a munkájuk során az információk biztonságos kezelése iránt. | | |
| **5 glosszárium bejegyzés** | | |
| **Kiberbiztonság.** Eszközök, technológiák, irányelvek, ellenőrzések és eljárások alkalmazása a hálózatok, rendszerek, eszközök és alkalmazások védelmére vagy helyreállítására a kibertámadásoktól, amelyek célja az érzékeny információkhoz való hozzáférés, azok megsemmisítése vagy megváltoztatása, a munkafolyamatok megzavarása vagy a szervezetek vagy egyének pénzének kicsikarása.  **Adathalászat.** Az a technika, amikor e-mailben egy másik személynek vagy szervezetnek adják ki magukat, és a felhasználót arra késztetik, hogy egy csalárd oldalon valamilyen műveletet hajtson végre jelszavak megszerzése vagy egy fertőzött fájl letöltése érdekében. Hasonló a vishing (hangalapú adathalászat) vagy a smishing (SMS + adathalászat).  **Malware.** Rosszindulatú szoftver, amely különböző formákban (futtatható kódként, szkriptek formájában stb.) jelenhet meg, és többek között olyan műveleteket végezhet, mint az érzékeny adatok titkosítása vagy törlése, az eszköz alapvető funkcióinak módosítása, a felhasználó tevékenységének kémkedése. A vírusok, férgek, reklámprogramok, trójaiak, kémprogramok és zsarolóprogramok szintén rosszindulatú programok.  **Biztonsági mentés.** Fájlok és programok másolata, amelyet más eszközökön vagy más adathordozókon tárolnak, hogy meghibásodás, elvesztés vagy lopás esetén helyreállítsák az információkat.  **Érzékeny információk.** Magánjellegű vagy bizalmas adatokat, például személyes vagy banki adatokat tartalmazó információk. | | |
| **Bibliográfia és további hivatkozások** | | |
| <https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-entorno-laboral-hibrido_20210928.html>  <https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-attacks-ebook-en-es.pdf>  <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>  <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>  <https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf>  <https://www.microfocus.com/en-us/what-is/cyber-security>  <https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer>  <https://es.linkedin.com/pulse/recomendaciones-de-ciberseguridad-en-el-puesto-trabajo-pizarro>  <https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html>  <https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/>  <https://uniserveit.com/blog/10-step-cybersecurity-plan-for-your-small-business>  <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes>  <https://www.europol.europa.eu/wannacry-ransomware> | | |
| **Öt feleletválasztós önértékelő kérdés**  Az érvényesítési mechanizmus befejezése után a felhasználók személyre szabott részvételi és teljesítési igazolást tudnak majd generálni. | | **Mit jelent a "kiberbiztonság"?**  a. Eszközök a készülékek védelmére a rosszindulatú szoftverek támadásaival szemben.  b. A bizalmas információk rosszindulatú támadásoktól való védelmét szolgáló eljárások.  c. A vállalati informatikai rendszerek védelme.  **d. Minden válasz helyes.**  **2. kérdés. Mit kell tennie az adathalászat megelőzése érdekében?**  **a. Óvakodjon a jelszó megváltoztatására vonatkozó kéretlen e-mailektől.**  b. Kattintson az e-mailekben található linkekre.  c. Töltse le a spam e-mailek mellékleteit.  d. Fogadja az ismeretlen számokról érkező telefonhívásokat.  **3. kérdés. Mi a leggyakoribb támadás az európai KKV-k ellen?**  a. Hozzáférés megtagadása.  b. Zsarolószoftver.  **c. Adathalászat.**  d. Egyik sem helyes.  **4. kérdés. Az alábbiak közül melyek az információkhoz való távoli hozzáférés kiberbiztonsági célkitűzései?**  **a. Hozzáférhetőség, bizalmasság.**  b. Nyomonkövethetőség, nyilvánosság.  c. Titoktartás, korrupció.  d. Integritás, mérhetőség.  **Mit tenne azzal az USB-meghajtóval, amit az irodai asztalon talál?**  a. Csatlakoztatja a számítógépéhez, hogy megnézze, mi van rajta és visszaadhassa a tulajdonosának.  **b. Megpróbálja megtalálni a tulajdonosát anélkül, hogy csatlakoztatja bármelyik számítógéphez.**  c. Jelenti a rendőrségnek.  d. Kidobja. |
| **Kapcsolódó anyagok** | | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_HU |
| **Hivatkozási link** | | - |
| **YouTube formátumú videó (ha van)** | | <https://www.youtube.com/watch?v=PSrnvEEDpuY> |