**Tréningový materiál**

|  |  |  |
| --- | --- | --- |
| **Názov** | | Kybernetická bezpečnosť v (home) office |
| **Kľúčové slová** | | Kybernetická bezpečnosť, bezpečnosť, malvér, phishing, citlivé informácie |
| **Autor** | | Internet Web Solutions |
| **Jazyk** | | Slovenský |
| **Tréningová oblasť** | | |
|  | Innovácie & Servitizácia | |
| **X** | Digitálna Transformácia | |
|  | Lokalizácia | |
|  | Udržateľnosť | |
| **Kompetencie a zručnosti podľa ESCO** | | |
| * Prierezové zručnosti a kompetencie   + Sociálne a emočné zručnosti   + Kritické myslenie   + Analytické myslenie   + Riešenie problémov   + Manažment seba samého   + Podnikový manažment   + Adaptabilia   + Odolnosť   + Kreativita   + Networking   + Iniciatíva   + Flexibilita   + Otvorenosť   + Pochopenie komplexnosti   + Spolupráca   + Empatia   + Inovácie   + Vodcovstvo / Leadership      * Zručnosti   + Technologické zručnosti   + Marketing produktu   + Digitálny marketing   + Digitálne zručnosti   + Komunikácia   + Spolupráca   + Emocionálna inteligencia      * Znalosti   + Podnikový manažment   + Online vzdelávanie   + Reklama   + Cloud computing   + Big dáta   + E-commerce   + Umelá inteligencia   + IoT (Internet vecí)   + Digitálna gramotnosť   + Kybernetická bezpečnosť   + Data mining a dátové analýzy   + Udržateľnosť   + Well-being   + Klimatická zmena   + Riadenie sociálnych médií | | |
| **Upútavka** | | |
| “Vedeli ste, že 85% európskych MMSP, považuje kybernetickú bezpečnosť za kľúčový problém ich podnikania?” | | |
| **Ciele / výsledky vzdelávania** | | |
| V tomto module sa dozviete čo je to kybernetická bezpečnosť, oboznámite sa s najčastejšie používanou terminológiou v tejto oblasti a zistíte niečo o najčastejších kybernetických útokoch počas práce z domu a z kancelárie. Budete tak schopný predchádzať hlavným kybernetickým rizikám a prehliadať internet bezpečne, nie len počas práce z domu, ale aj počas vykonávania každodenných aktivít na internete, čím zvýšite svoje znalosti a zručnosti o počítačovej bezpečnosti. | | |
| **Popis** | | |
| Väčšina európskych MMSP vnímajú kybernetickú bezpečnosť ako kľúčový problém podnikania. V postpandemickom kontexte, však nie všetky spoločnosti implementovali nové bezpečnostné opatrenia v boji proti rizikám vznikajúcim pri práci na diaľku v dôsledku nedostatočného povedomia a nedostatku zručností v oblasti kybernetickej bezpečnosti. Tento modul umožní zamestnancom a podnikateľom v MMSP zlepšiť svoje zručnosti a znalosti v oblasti kybernetickej bezpečnosti, aby zvýšili ich digitálne zručnosti a kybernetickú odolnosť. | | |
| **Zoznam výhod pre podnikateľov** | | |
| ✓ Implementácia stratégií kybernetickej bezpečnosti v MMSP znižuje riziko straty a úniku informácií pri zachovávaní integrity údajov.  ✓ Udržiavaním informácií o zákazníkoch v tajnosti/bezpečnosti sa povesť a imidž spoločnosti zlepšuje aj v očiach verejnosti.  ✓ Kybernetická bezpečnosť zvyšuje odolnosť a kapacitu obnovy dát v spoločnosti pomocou zálohovania, ktoré im umožňuje obnoviť stratené súbory po nečakanom útoku.  ✓ Znižovaním straty informácií kvôli kybernetickým útokom alebo interným problémom sa zvyšuje produktivita.  ✓ Kybernetická bezpečnosť je nevyhnutným nástrojom pre zamestnávateľov a zamestnancov v pracovnom aj v osobnom živote, kvôli narastajúcim kybernetickým rizikám (napr. v online nakupovaní). | | |
| **Obsah usporiadaný do 3 úrovní** | | |
| **Modul: Kybernetická bezpečnosť v (home) office**  **Kapitola 1: Základy kybernetickej bezpečnosti**  **Sekcia 1.1: Čo je kybernetická bezpečnosť?**  Pojem „**kybernetická bezpečnosť**" sa zrodil v 70-tych rokoch 20. storočia, keďže spoločnosti potrebovali **chrániť svoje počítačové systémy** pred škodlivými útokmi, ktoré by zneužitím informácií mohli ohroziť ich správne fungovanie.  Kybernetická bezpečnosť zahŕňa aplikáciu nástrojov, technológií, politík, kontrol a postupov na ochranu alebo obnovu sietí, systémov, zariadení a aplikácií pred **kybernetickými útokmi** zameranými na prístup, zničenie či zmenu citlivých informácií, narušenie pracovných tokov, alebo vymáhanie peňazí od organizácií alebo jednotlivcov.  Podľa správy Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) z roku 2021, **85%** z 249 opýtaných európskych mikro, malých a stredných podnikov (MMSP), **považuje kybernetickú bezpečnosť za kľúčový problém ich podnikania**. V post-pandemickom kontexte, 45% MMSP implementovalo nové technológie ako reakciu na pandémiu, no 90% nezahrnulo súvisiace bezpečnostné opatrenia.  Uvedená správa poskytuje hodnotné informácie o kybernetickej bezpečnosti európskych MMSP a poukazuje tiež na **hlavné kyberbezpečnostné prípady, ktorým čelia Európske** MMSP **na základe ich pôvodu**, ako je znázornené na grafe.  Zdroj: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> (vlastné spracovanie)  **Sekcia 1.2: Hlavné definície**  Bezpečnosť vo všeobecnosti:   * **Zálohovanie:** kópia súborov a programov, ktorá je uložená na iných zariadeniach alebo médiách, s cieľom obnoviť informácie v prípade zlyhania, straty alebo krádeže. * **Citlivé informácie**: informácie obsahujúce citlivé, resp. dôveryhodné údaje, ako napríklad bankové či osobné informácie. * **Softvér**: softvér je počítačový program určený na vykonávanie špecifických úloh, napríklad internetový prehliadač, hra, a pod. Je to protiklad "hardvéru", ktorý sa skladá z fyzických komponentov zariadenia, ako sú základná doska a procesor. * **Šifrovanie**: je proces, ktorý konvertuje dokument alebo súbor na informácie, ktoré sú nečitateľné pre ľudí, ktorí nemajú kľúč na ich dešifrovanie. Slúži na ochranu informácií pred ľuďmi, ktorí by k nim nemali mať prístup. * **HTTP / HTTPS**: jeden z najpoužívanejších protokolov na prehliadanie internetu. HTTPS (HyperText Transfer Protocol Secure) je zabezpečená verzia a zaisťuje, aby prenos informácií medzi vašim zariadením a webovou stránkou bol šifrovaný a chránený. * **Firewall**: počas prehliadania webu a pristupovania na webovú stránku, komunikuje s vašim počítačom, aby nadviazala spojenie. Firewall analyzuje tento typ prepojenia, aby predchádzala prístupu k takým internetovým stránkam, ktoré by mohli predstavovať riziko.   Hrozby:   * **Sciálne inžinierstvo**: sociálne inžinierstvo si nevyžaduje veľkú úroveň počítačových zručností, pretože zahŕňa manipuláciu ľudí prostredníctvom psychologických techník a sociálnych zručností, a je často používané na získanie citlivých informácií ako sú heslá, či bankové údaje. Techniky phishingu sú založené na sociálnom inžinierstve. * **Phishing**: technika vydávania sa za inú osobu alebo subjekt prostredníctvom e-mailu, ktorá vedie používateľa k vykonaniu určitej akcie na podvodnej stránke s cieľom získať heslá alebo stiahnuť infikovaný súbor. * **Smishing**: SMS + phishing. Podobné phishingu, táto technika používa SMS správy na ten istý účel. * **Vishing**: hlas + phishing. V tomto prípade, útočník predstiera, že je niekto iný počas hovoru cez telefón. Často sa vydáva za technickú podporu zariadenia alebo telefonickú spoločnosť. * **Webové útoky**: tieto komplexné útoky pri používaní internetu využívajú škodlivý softvér na infikovanie zariadení, ktoré nemajú potrebné zabezpečenie alebo sú zastarané.   Typy malvérov:   * **Malvér**: malvér je škodlivý softvér, ktorý môže mať rôzne formy (ako spustiteľný kód, script, a pod.), a môže vykonávať akcie ako je šifrovanie alebo odstraňovanie citlivých údajov, pozmenenie základných funkcií zariadenia, špehovanie aktivity používateľa a ďalšie. Anti-malware je softvér, ktorého funkciou je detegovať, chrániť a odstraňovať tento typ škodlivých softvérov. Existuje veľa typov malvéru, ktoré si priblížime na nasledujúcich slajdoch. * **Počitačový vírus**: tento typ malvéru má za cieľ zmeniť fungovanie zariadenia a vyžaduje interakciu užívateľa na šírenie ďalších súborov a systémov. * **Počítačový červ**: dokáže sa replikovať a prenášať z infikovaného zariadenia na iné zariadenia prostredníctvom siete. Často pochádza z infikovaných USB jednotiek, príloh e-mailov, či dokonca webových stránok. * **Trójsky kôň**: tento typ malvéru vstupuje do systému ako neškodný súbor alebo softvér a vykonáva nechcené akcie na pozadí, ako je mazanie súborov alebo sťahovanie iného malvéru. * **Spyware**: ako naznačuje názov, tento typ malvéru špehuje infikované zariadenie tak, že zbiera informácie o aktivite používateľa. Zvyčajne pochádza zo spamu alebo podvodných webstránok na sťahovanie. * **Adware**: malvér, ktorý sleduje prehliadač používateľa a sťahuje históriu aby zobrazoval nechcené reklamy alebo bannery, na ktoré môže používateľ kliknúť. Zvyčajne infikujú zariadenia prostredníctvom infikovaných webových stránok alebo podvodných webstránok určených na sťahovanie súborov. * **Ransomware**: nebezpečný typ malvéru, ktorý šifruje súbory na pevnom disku zariadenia a obmedzuje prístup používateľovi, pričom vyžaduje výkupné, zvyčajne v kryptomenách, ako výmenu za dešifrovanie súborov. Známym prípadom je [**WannaCry**](https://www.europol.europa.eu/wannacry-ransomware).   **Kapitola 2: Kybernetická bezpečnosť…**  **Sekcia 2.1: …** **na pracovisku**  **Kybernetická bezpečnosť v spoločnosti je zodpovednosťou každého**, tak manažmentu, ako aj zamestnancov. Preto musí byť súčasťou pracovnej kultúry spoločnosti.  Nielen na pracovisku ale aj doma je naozaj nevyhnutné dodržiavať **sériu základných opatrení v rámci plánu kybernetickej bezpečnosti** pre správne fungovanie podnikania.  Prečítajte si, ktoré opatrenia v rámci základného plánu kybernetickej bezpečnosti je potrebné dodržiavať, aby sa zachovala integrita informácií spoločnosti:   * **Informujte o zásadách kybernetickej bezpečnosti vo vašej spoločnosti.** Každá spoločnosť má jedinečné potreby, a preto by mali byť zásady kybernetickej bezpečnosti tvorené v jej konkrétnych podmienkach a dodržiavané všetkými zamestnancami a manažérmi, aby sa vytvorila kultúra kybernetickej bezpečnosti. * **Aktualizujte softvér vo vašich zariadeniach.** Udržiavaním aktuálnosti všetkých aplikácií a operačných systémov sa predchádza ich zraniteľnostiam. * **Nastavte firewall.** Firewall poskytne dodatočnú ochranu počas prehliadania internetu. * **Pravidelne zálohujte.** V prípade straty údajov, vám zálohovanie pomôže rýchlo obnoviť pôvodný stav. * **Zabezpečte wifi sieť.** Wifi siete používané pri každodennej aktivite by mali byť správne nakonfigurované tak, aby boli dostatočne zabezpečené proti tretím stranám. * **Nainštalujte anti-malvérový softvér** na ochranu proti možným útokom. * **Vytvorte akčný plán pre mobilné zariadenia.** Kybernetická bezpečnosť nie je iba pre počítače, ale aj pre mobilné zariadenia ako sú smartfóny a tablety, ktoré musia byť tiež chránené. * Zaveďte postupy na ochranu informácií, ktoré sa majú dodržiavať v prípade kyberbezpečnostného útoku. * **Používajte silné heslá.** Tie by mali obsahovať čísla, písmená a špeciálne znaky. Jedným zo spôsobov ako zistiť, či sú heslá bezpečné je ich kontrola na webovej stránke <https://password.kaspersky.com/>. * **Obmedzte povolenia na inštaláciu softvéru.** Zamestnanci by mali mať obmedzený prístup k inštalácii nových softvérov, aby sa predchádzalo inštalácii podvodných aplikácií, ktoré by mohli infikovať sieť zariadení.   **Sekcia 2.2: …** **pri práci na diaľku**  **Pri práci na diaľku je kybernetická bezpečnosť ešte dôležitejšia**, pretože pri práci z domu nie je rovnaká kontrola politík a postupov kybernetickej bezpečnosti spoločnosti, siete sú menej zabezpečené, okrem iného môžu nastať konfiguračné chyby, alebo nedostatočné školenia.  Z dôvodu rozdielnej kontroly kybernetickej bezpečnosti; nižšej zabezpečenosti sietí; konfiguračných chýb, či nedostatočných poznatkov je potrebné zvážiť **také opatrenia kybernetickej bezpečnosti, ktoré zabezpečia splnenie nasledovných cieľov získavania informácií pri práci na diaľku:**   * **Dostupnosť.** Oprávnení užívatelia musia mať v prípade potreby prístup k informáciám. * **Dôveryhodnosť.** Iba oprávnení užívatelia môžu mať prístup k informáciám. * **Autentickosť.** Oprávnení užívatelia (s prístupom k informáciám) sú tými, za ktorých sa vydávajú. * **Dohľadateľnosť.** Musí byť možne sledovať neplatný alebo neautorizovaný prístup k informáciám. * **Integrita.** Informácie a metódy ich spracovania sú presné a úplné.   Okrem spomínaného plánu kybernetickej bezpečnosti sa výrazne odporúča využívať **VPN** (**Virtual Private Network**). Táto sieťová technológia umožňuje zabezpečenie medzi lokálnou sieťou a internetom tak, aby bola **zaručená integrita a dôveryhodnosť informácií**.  Okrem iného, **aplikácie pre vzdialený prístup na plochu** umožnia pracovníkom ovládať na diaľku počítače, ktoré sa fyzicky nachádzajú na pracovisku. Takým je aj nástroj TeamViewer.  **Cloudové riešenia** a **kolaboratívne nástroje** sú tiež dôležité nástroje pre kybernetickú bezpečnosť pri práci na diaľku, ktoré **umožňujú rýchly a koordinovaný prístup k informáciám**.  Príklady nástrojov pri práci na diaľku:  **VPN:**   * **hide.me.** Táto VPN služba umožňuje súkromne prehliadať internet bez geografických obmedzení. Ráta s viac ako 2000 servermi a 75 lokáciami. <https://hide.me/> * **PrivadoVPN.** založená vo Švajčiarsku. Jej bezplatná verzia umožňuje chrániť až 10 GB dát každý mesiac. <https://privadovpn.com/>   **Vzdialená pracovná plocha:**   * **AnyDesk.** Je ďalším softvérom pre vzdialenú pracovnú plochou, ktorý je tiež dostupný bezplatne pre osobné využívanie. Tento typ nástroja umožňuje prístup k informáciám kdekoľvek, čo zlepšuje internú komunikáciu. <https://anydesk.com/> * **TeamViewer.** Tento nástroj sa zameriava viac na vzdialený prístup k informáciám. Umožňuje prístup k akémukoľvek zariadeniu z akéhokoľvek miesta. Umožňuje zabezpečenie zdieľania súborov a prístup k iným zariadeniam, a je bezplatný pre osobné využívanie. <https://www.teamviewer.com/>   **Cloudové riešenia:**   * **Dropbox.** Bezplatná verzia poskytuje 2 GB úložisko a platená verzia môže poskytnúť úložisko až do 3 TB. <https://www.dropbox.com/> * **MEGA.** Táto platforma zahŕňa 20 GB zadarmo. Poskytuje platenú verziu pre jednotlivcov až do 16 TB a pre spoločnosti do 10 PB, čo ju čo ju zaraďuje medzi poskytovateľov cloudových riešení s najväčšou kapacitou. <https://mega.io/>   **Kolaboratívne nástroje:**   * **Slack.** Táto platforma okamžitých správ umožňuje integráciu s inými nástrojmi a zjednodušuje tímovú komunikáciu. Bezplatná verzia umožňuje prístup k histórii až posledných 10 000 správ tímu, video hovorov s kolegami, a integruje sa s 10 aplikáciami. <https://slack.com/> * **Trello.** Tento nástroj pracuje so systémom kariet Kanban a umožňuje používateľovi vkladať do systému poznámky, súbory, deadliny a ďalšie položky. Ľahko sa spravuje potiahnutím kariet a je dostupný v niekoľkých jazykoch. Tento nástroj je bezplatný v počte 10 projektov pre tím. <https://trello.com/>   **Kapitola 3: Odporúčania pre podnikateľov a zamestnancov**  **Sekcia 3.1: Odporúčania pre podnikateľov**   * Uistite sa, že vaša spoločnosť má **plán kybernetickej bezpečnosti,** ktorý je vhodný pre vaše potreby a potenciálne zraniteľné miesta vášho podnikania. * Formulujte zásady a postupy pre **manažment zabezpečenia informácií**, napr. žiadne osobné zariadenia, bezpečné zničenie dokumentov a pod. * **Vyškoľte svojich zamestnancov v oblasti kybernetickej bezpečnosti,** aby mohli dodržiavať vami naformulované zásady a postupy. * **Zlepšite vaše digitálne zručnosti v oblasti kybernetickej bezpečnosti.** Pamätajte, že narábate s veľmi citlivými informáciami. * Dodržujte aj **odporúčania pre zamestnancov** definované na nasledovnom slajde! J   **Sekcia 3.2: Odporúčania pre zamestnancov**   * Kybernetická bezpečnosť začína **fyzickým zabezpečením informácií**: udržujte svoju pracovnú plochu bez dôverných informácií, hesiel, e-mailov a pod. * Nepripájajte **USB zariadenia** od nedôveryhodných ľudí, pretože môžu infikovať váš počítač. * **Šifrujte citlivé informácie pred ich odoslaním**, napr. cez komprimovaný súbor chránený heslom. * Pamätajte na pravidelné “**vysypávanie“ koša v počítači**. * Pravidelne **zálohujte**. * **Chráňte citlivé informácie vo vašich mobilných zariadeniach** aj mimo práce. * Ak je to možné, **vyhnite sa pripájaniu na otvorené siete wifi** s pracovnými zariadeniami. Ak to potrebujete spraviť, použite VPN pre zabezpečenie. * **Uzamknite pracovnú plochu vášho počítača** keď odchádzate od pracovného stolu. * Používajte **bezpečné heslá**. Overiť si bezpečnosť vašich hesiel môžete napríklad na webovej stránke <https://password.kaspersky.com/> vyhradenej pre kontrolu hesiel. * **Nepoužívajte vždy tie isté heslá**, pretože budete viac zraniteľní v prípade ich úniku. * **Nesťahujte prílohy od neznámych odosielateľov**, dávajte si pozor na **podozrivé správy** a **nahláste akékoľvek útoky** svojim nadriadeným. | | |
| **Obsah v bodoch** | | |
| * Kybernetická bezpečnosť vznikla z potreby spoločností chrániť ich počítačové systémy pred kybernetickými útokmi. * Najčastejšie útoky, ktoré zasahovali európske MMSP súviseli s phishingom. * Kybernetická bezpečnosť je zodpovednosť každého v spoločnosti. Preto je nevyhnutné mať plán kybernetickej bezpečnosti, ktorý je dôsledne dodržiavaný manažérmi, riaditeľmi a zamestnancami. * Pri práci na diaľku je kybernetická bezpečnosť doplnená o používanie nástrojov informačno-komunikačných technológií (IKT), ktoré umožňujú dosiahnuť päť cieľov kybernetickej bezpečnosti pri prístupe k informáciám. * Zamestnávateľ musí zabezpečiť, aby bol zavedený plán kybernetickej bezpečnosti, a aby zamestnanci mali potrebné zručnosti na jeho dodržiavanie. * Zamestnanci by sa mali počas svojej práce zaviazať k bezpečnému spravovaniu informácií. | | |
| **5 slovníkových pojmov** | | |
| **Kybernetická bezpečnosť.** Aplikácia technológií, politík, kontrol a postupov na ochranu alebo obnovu sietí, systémov, zariadení a aplikácií pred **kybernetickými útokmi** zameranými na prístup, zničenie, či zmenu citlivých informácií, narušenie pracovných tokov, alebo vymáhanie peňazí od organizácií alebo jednotlivcov.  **Phishing.** Technika vydávania sa za inú osobu alebo subjekt prostredníctvom e-mailu, ktorá vedie používateľa k vykonaniu určitej akcie na podvodnej stránke s cieľom získať heslá alebo stiahnuť infikovaný súbor. Podobnými sú vishing (hlas + phishing) alebo smishing (SMS + phishing).  **Malvér.** Škodlivý softvér, ktorý môže mať rôzne formy (ako spustiteľný kód, script, atď.), a môže vykonávať akcie ako je šifrovanie alebo odstraňovanie citlivých údajov, pozmenenie základných funkcií zariadenia, špehovanie aktivity používateľa a ďalšie. Vírusy, počítačové červy, adware, trójske kone, spyware a ransomware patria medzi malvéry.  **Zálohovanie.** Kópia súborov a programov, ktorá je uložená na iných zariadeniach alebo médiách, s cieľom obnoviť informácie v prípade zlyhania, straty alebo krádeže.  **Citlivé informácie.** Informácie obsahujúce súkromné alebo dôveryhodné údaje, ako sú osobné či bankové údaje. | | |
| **Bibliografia a ďalšie odkazy** | | |
| <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> | | |
| **Päť kvízových otázok s možnosťou výberu odpovede**  Po dokončení kvízu s minimom 75 % správnych odpovedí si budú môcť používatelia vygenerovať personalizovaný certifikát o účasti a absolvovaní tréningu. | | **Otázka 1. Čo znamená „kybernetická bezpečnosť"?**  Možnosť a: Ide o súbor nástrojov na ochranu zariadení pred malvérovými útokmi.  Možnosť b: Predstavuje postupy navrhnuté na ochranu citlivých informácií pred malvérovými útokmi.  Možnosť c: Predstavuje ochranu IT systémov spoločnosti.  Možnosť d: Všetky možnosti sú správne.  **Správna možnosť: d**  **Otázka 2. Čo by ste mali robiť aby ste predišli phishingu?**  Možnosť a: Dávať si pozor na nevyžiadané e-maily na zmenu hesla.  Možnosť b: Kliknúť na linky v e-mailoch.  Možnosť c: Sťahovať prílohy spamových emailov.  Možnosť d: Brať telefonické hovory od neznámych čísel.  **Správna možnosť: a**  **Otázka 3. Aký je najčastejší útok na európske MMSP?**  Možnosť a: Odmietnutie služby.  Možnosť b: Ransomware.  Možnosť c: Phishing.  Možnosť d: Žiadna možnosť nie je správna.  **Správna možnosť: c**  **Otázka 4. Ktorá z možností uvádza ciele kybernetickej bezpečnosti pre vzdialený prístup k informáciám?**  Možnosť a: Dostupnosť, dôveryhodnosť.  Možnosť b: Dohľadateľnosť, publicita.  Možnosť c: Dôveryhodnosť, korupcia.  Možnosť d: Integrita, merateľnosť.  **Správna možnosť: a**  **Otázka 5. Čo by ste robili s USB diskom, ktorý nájdete na pracovnom stole?**  Možnosť a: Pripojil by som ho do svojho počítača, aby som zistil, čo je na ňom a tak ho mohol vrátiť jeho majiteľovi.  Možnosť b: Snažil by som sa ho vrátiť jeho majiteľovi bez toho, aby som ho pripojil do počítača.  Možnosť c: Nahlásil by som to polícii.  Možnosť d: Zahodil by som ho.  **Správna možnosť: b** |
| **Súvisiaci materiál** | | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_EN.pptx |
| **Referenčné odkazy** | | - |
| **Video vo formáte Youtube** | | <https://www.youtube.com/watch?v=PSrnvEEDpuY> |