**Opis/sadržaj edukacije**

|  |  |  |
| --- | --- | --- |
| **Naslov** | | Kibernetička sigurnost u poslovanju |
| **Ključne riječi (meta element)** | | kibernetička sigurnost, sigurnost, *malware*, *phishing*, osjetljive informacije |
| **Izradio/la** | | Internet Web Solutions |
| **Jezik** | | Hrvatski |
| **Područja edukacije (X – primjenjivo)** | | |
|  | Inovacija i servitizacija | |
| **X** | Digitalna transformacija | |
|  | Lokalizacija | |
|  | Održivost | |
| **ESCO kompetencije i vještine** | | |
| * Transverzalne vještine i kompetencije   + Društvene i emocionalne vještine   + Kritičko razmišljanje   + Analitičko razmišljanje   + Rješavanje problema   + Samoupravljanje   + Poslovno upravljanje   + Prilagodljivost   + Otpornost   + Kreativnost   + Umrežavanje   + Inicijativa   + Fleksibilnost   + Otvorenost   + Razumijevanje složenih problema   + Suradnja   + Suosjećanje   + Inovacija   + Vodstvo * Vještine   + Tehnološke vještine   + Marketing proizvoda   + Digitalni marketing   + Digitalne vještine   + Komunikacija   + Suradnja   + Emocionalna inteligencija * Znanje   + Poslovno upravljanje   + Online učenje i obuka   + Oglašavanje   + Računarstvo u oblaku   + Veliki podaci   + E-trgovina   + Umjetna inteligencija   + Internet stvari (IoT)   + Digitalna pismenost   + Kibernetička sigurnost   + Rudarenje i analiza podataka   + Održivost   + Dobrobit   + Klimatske promjene   + Upravljanje društvenim mrežama | | |
| **Teaser** | | |
| “Jeste li znali da 85% europskih mikro, malih i srednjih poduzeća (MSMEs) smatra kibernetičku sigurnost ključnom brigom za svoje poslovanje?” | | |
| **Ciljevi / ishodi učenja** | | |
| U ovom modulu naučit ćete što je kibernetička sigurnost, upoznati se s najčešće korištenom terminologijom i saznati koji su najčešći kibernetički napadi pri radu od kuće i iz ureda. Na taj ćete način moći izbjeći glavne kibernetičke rizike, čime poboljšavate svoje vještine i znanje o računalnoj sigurnosti. | | |
| **Opis** | | |
| Većina europskih mikro, malih i srednjih poduzeća kibernetičku sigurnost vidi kao ključnu brigu za svoje poslovanje. Međutim, nakon Covid pandemije, nisu sva poduzeća implementirala nove sigurnosne mjere za borbu protiv rizika koji proizlaze iz rada na daljinu, uglavnom zbog nedostatka svijesti i vještina vezanih za kibernetičku sigurnosti. Ovaj modul omogućit će zaposlenicima mikro, malih i srednjih poduzeća te poduzetnicima da poboljšaju svoje vještine i znanja o kibernetičkoj sigurnosti čime će poboljšati svoje digitalne vještine i kibernetičku otpornost. | | |
| **Popis benefita za poduzetnike** | | |
| ✓ Provedba strategija kibernetičke sigurnosti u mikro, malim i srednjim poduzećima smanjuje rizik od gubitka i curenja informacija, a istovremeno održava integritet podataka.  ✓ Čuvanjem povjerljivih informacija o kupcima, povećava se i ugled poduzeća te korporativni imidž.  ✓ Kibernetička sigurnost povećava otpornost i kapacitet oporavka poduzeća, uz sigurnosne kopije koje omogućuju nastavak poslovanja nakon neočekivanog incidenta.  ✓ Smanjenjem gubitka informacija zbog kibernetičkih napada ili internih problema, dolazi i do povećanja produktivnosti.  ✓ Kibernetička sigurnost bitan je alat za poslodavce i zaposlenike, ne samo u poslovnom nego i u osobnom životu, podizanjem svijesti i sprječavanjem kibernetičkih rizika (npr. u online kupovini). | | |
| **Sadržaj raspoređen u 3 razine** | | |
| **Modul: Kibernetička sigurnost**  **Dio 1: Osnove kibernetičke sigurnosti**  **Odjeljak 1.1: Što je kibernetička sigurnost?**  Pojam "***cybersecurity***“ odnosno kibernetička sigurnost nastao je 1970-ih zbog potrebe poduzeća da **zaštite svoje računalne sustave** od zlonamjernih napada mogli ugroziti njihovo funkcioniranje.  Kibernetička sigurnost uključuje primjenu alata, tehnologija, politika, kontrola i postupaka u zaštiti ili oporavku mreža, sustava, uređaja i aplikacija od **kibernetičkih napada** koji su usmjereni na pristup, uništavanje ili mijenjanje osjetljivih informacija, ometanje tijeka rada ili iznuđivanje novca od organizacija ili pojedinaca.  Prema izvješću Agencije Europske unije za kibernetičku sigurnost (ENISA) iz 2021., od ukupno 249 ispitanih europskih mikro, malih i srednjih poduzeća, njih **85% smatra da je kibernetička sigurnost ključna briga za njihovo poslovanje**. Nakon pandemije, 45% mikro, malih i srednjih poduzeća implementiralo je u svoje poslovanje nove tehnologije kao odgovor na pandemiju, no 90% nije u to uključilo nove sigurnosne mjere.  Isto izvješće, koje pruža važne informacije o kibersigurnosti, prikazuje **glavne sigurnosne incidente koje su pretrpjela europska mikro, mala i srednja poduzeća**. Incidenti su prikazani na  grafikonu.    Izvor: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>  **Odjeljak 1.2: Glavne definicije**  Opća sigurnost:   * **Sigurnosna kopija**: Kopija datoteka i programa koja je pohranjena na drugim uređajima ili drugim medijima, koja omogućava povrat informacija u slučaju kvara, gubitka ili krađe * **Osjetljive informacije:** Informacije koje sadrže privatne ili povjerljive podatke, poput osobnih ili bankovnih podataka. * **Softver**: Softver je računalni program dizajniran za obavljanje specifičnih zadataka, na primjer internet preglednik, igra itd. Suprotan je od hardvera, koji se odnosi na fizičke komponente, kao što su matična ploča ili procesor. * **Enkripcija**: Proces koji pretvara dokument ili datoteku u informacije koje nisu čitljive osobama koje nemaju ključ za dešifriranje. Služi za zaštitu informacija od osoba koje im ne bi trebale imati pristup. * **HTTP / HTTPS:** Jedan od najčešće korištenih protokola za pregledavanje interneta. HTTPS (HyperText Transfer Protocol Secure) je sigurna inačica i osigurava da su informacije koje se prenose između vašeg uređaja i web stranice šifrirane i zaštićene. * **Vatrozid**: Tijekom pretraživanja interneta i pristupanja web stranici, komunicira s vašim računalom kako bi uspostavio vezu. Vatrozid analizira ovu vrstu veze kako bi spriječio pristup onima koji bi mogli predstavljati rizik.   Prijetnje:   * **Socijalni inženjering**: Socijalni inženjering ne zahtijeva visoke računalne vještine, budući da uključuje manipulaciju ljudima putem psiholoških tehnika i društvenih vještina. Često se koristi za dobivanje osjetljivih informacija, poput lozinki ili bankovnih podataka. Tehnike krađe identiteta temelje se na socijalnom inženjeringu. * ***Phishing***: Korisnik dobiva e-poštu koja ga navodi da izvrši neku radnju na lažnoj web stranici, da npr. upiše svoju lozinku ili preuzme zaraženu datoteku. * ***Smishing***: SMS + *phishing*. Slično *phishingu*, ova tehnika koristi SMS poruke za istu svrhu. * ***Vishing***: Glas + phishing. U ovom slučaju, napadač se pretvara da je netko drugi tijekom telefonskog razgovora (najčešće korisnička podrška) i pokušava na taj način doći do povjerljivih informacija. * **Napadi na webu**: Tijekom pretraživanja interneta zlonamjerni softver napada uređaje koji su zastarjeli ili nemaju aktivirane adekvatne mjere zaštite.   Vrste *malwarea*:   * ***Malware***: *Malware* je zlonamjerni softver koji može imati različite oblike (kod, skripta itd.) i može izvoditi radnje kao što su šifriranje ili brisanje osjetljivih podataka, mijenjanje osnovnih funkcija uređaja, špijuniranje aktivnosti korisnika itd. *Anti-malware* je softver čija je funkcija otkriti, zaštititi i ukloniti ovu vrstu zlonamjernog softvera. * **Računalni virus**: Ova vrsta zlonamjernog softvera ima za cilj promijeniti funkcioniranje uređaja i zahtijeva interakciju korisnika za širenje na druge datoteke i sustave. * **Računalni crv**: Može se replicirati i premještati s jednog zaraženog uređaja na drugi diljem mreže. Često dolazi sa zaraženih USB uređaja, privitaka e-pošte ili čak web stranica. * **Trojan**: Ova vrsta zlonamjernog softvera ulazi u sustav kao bezopasna datoteka ili softver i izvodi neželjene radnje u pozadini, poput brisanja datoteka ili preuzimanja drugog zlonamjernog softvera. * ***Spyware***: Kao što naziv sugerira, ova vrsta zlonamjernog softvera špijunira zaraženi uređaj, prikupljajući podatke o aktivnosti korisnika. Obično dolazi iz neželjene e-pošte (spama) ili preuzimanja lažnih datoteka. * ***Adware***: *Malware* koji prati korisnikov internet preglednik i povijest preuzimanja kako bi prikazao neželjene oglase ili *bannere* na koje korisnik može kliknuti. Obično zaraze uređaje putem zaraženih web stranica ili web stranica za preuzimanje lažnih datoteka. * ***Ransomware***: Opasna vrsta zlonamjernog softvera koji šifrira datoteke na tvrdom disku uređaja i ograničava pristup korisniku, zahtijevajući otkupninu, obično u kriptovalutama, u zamjenu za dekriptiranje datoteka. Dobro poznat slučaj je [**WannaCry**](https://www.europol.europa.eu/wannacry-ransomware).   **Dio 2: Kibernetička sigurnost…**  **Odjeljak 2.1: …na radnom mjestu**  **Kibernetička sigurnost odgovornost je svih u poduzeću**, kako uprave tako i zaposlenika, stoga mora biti i dio radne kulture poduzeća.  Kako u uredu tako i kod kuće, potrebno je pridržavati se niza **osnovnih mjera u okviru plana kibernetičke sigurnosti** kako bi se osiguralo nesmetano odvijanje poslovanja.  U nastavku slijedi **osnovni plan kibernetičke sigurnosti** koji je potrebno slijediti kako bi se održao integritet informacija poduzeća:   1. **Informirajte se o politici kibernetičke sigurnosti poduzeća**. Svako poduzeće ima jedinstvene potrebe, stoga bi politika kibernetičke sigurnosti trebala biti razvijena i trebali bi ju slijediti zaposlenici i menadžeri kako bi se stvorila kultura kibernetičke sigurnosti. 2. **Ažurirajte softvere uređaja**. Održavanje svih aplikacija i operativnih sustava ažuriranim smanjuje njihovu ranjivosti. 3. **Postavite vatrozida**. Vatrozid će pružiti dodatnu zaštitu pri pretraživanju interneta 4. **Redovito radite sigurnosne kopije.** U slučaju gubitka podataka, sigurnosne kopije omogućit će brzo vraćanje poslovanja u normalu. 5. **Osigurajte wifi mreže**. Wifi mreže koje se koriste u svakodnevnim aktivnostima moraju biti ispravno konfigurirane kako bi bile dovoljno sigurne od trećih strana. 6. **Instalirajte *anti-malware* softver** radizaštite od mogućih napada. 7. **Definirajte akcijski plan za mobilne uređaje**. Kibernetička sigurnost ne odnosi se samo na računala, već i na mobilne uređaje poput pametnih telefona i tableta, koji također moraju biti zaštićeni. 8. **Implementirajte postupke za zaštitu informacija**. Definirajte korake kojih se treba pridržavati u slučaju kibernetičkih napada.      1. **Koristite jake lozinke.** Lozinke trebaju sadržavati brojeve, slova i posebne znakove. Jedan od načina da provjerite jesu li lozinke dovoljno jake je web stranica <https://password.kaspersky.com/>. 2. **Ograničite mogućnosti instalacije softvera**. Zaposlenici bi trebali imati ograničenu mogućnost instaliranja novih softvera, kako bi se spriječilo instaliranje lažnih aplikacija koje bi mogle zaraziti mrežne uređaje.   **Odjeljak 2.2: …u radu na daljinu**  **U radu na daljinu, kibernetička sigurnost je još važnija**, jer ne postoji ista količina kontrole nad kibernetičkim procedurama i politikama poduzeća, mreže su manje sigurne, može doći do pogrešaka u konfiguraciji itd.  Zbog toga se moraju razmotriti nove mjere kako bi se osiguralo postizanje sljedećih **ciljeva kibernetičke sigurnosti** za daljinski pristup informacijama:   * **Dostupnost**. Ovlašteni korisnici moraju imati pristup informacijama kada je to potrebno. * **Povjerljivost**. Mora se osigurati da samo ovlašteni korisnici mogu pristupiti informacijama. * **Autentičnost**. Mora se osigurati da su ovlašteni korisnici (s pristupom informacijama) oni za koje se predstavljaju. * **Sljedivost**. Mora postojati mogućnost praćenja nepropisnog ili neovlaštenog pristupa informacijama. * **Cjelovitost**. Mora se osigurati da su informacije i metode njihove obrade točne i potpune.   Uz prethodno spomenuti plan kibernetičke sigurnosti, korištenje **VPN-a (Virtual Private Network)** je također preporučljivo. Ova mrežna tehnologija omogućuje sigurnu vezu između lokalne mreže i interneta, **čime je zajamčena cjelovitost i povjerljivost podataka**.  Osim toga, **aplikacije za daljinski pristup računalu** omogućit će zaposlenicima da na daljinu upravljaju računalima koja se fizički nalaze u uredu. Primjer takvog alata je TeamViewer.  **Rješenja u oblaku te alati za suradnju i komunikaciju** također su važni alati za kibernetičku sigurnost u radu na daljinu, **omogućujući pristup informacijama na brz i koordiniran način**.  Primjeri alata za rad na daljinu:  **VPN:**   * **hide.me**. Ova VPN usluga omogućuje pretraživanje interneta na privatan način, bez geografskih ograničenja. <https://hide.me/> * **PrivadoVPN**. Sa sjedištem u Švicarskoj, besplatna verzija omogućuje zaštitu do 10 GB podataka svaki mjesec. <https://privadovpn.com/>   **Daljinski pristup računalu:**   * **AnyDesk**. Besplatan za osobnu upotrebu, omogućava pristup informacijama s bilo kojeg mjesta. <https://anydesk.com/> * **TeamViewer**. Ovaj se alat više fokusira na daljinski pristup informacijama jer omogućuje pristup bilo kojem uređaju s bilo kojeg mjesta. Osim toga, osigurava sigurno dijeljenje datoteka i pristup drugim uređajima, a besplatan je za osobnu upotrebu. <https://www.teamviewer.com/>   **Rješenja u oblaku:**   * **Dropbox**. Besplatni plan nudi 2 GB prostora za pohranu, a uz plaćanje moguće je koristiti do 3 TB prostora za pohranu. <https://www.dropbox.com/> * **MEGA**. Ova platforma uključuje 20 GB besplatnog prostora, plaćeni paketi za osobnu upotrebu do 16 TB, a za poduzeća do 10 PB, što je čini jednim od rješenja s najvećim kapacitetom. <https://mega.io/>   **Alati za suradnju i komunikaciju:**   * **Slack**. Ova platforma za razmjenu poruka omogućuje integraciju s drugim alatima i pojednostavljuje timsku komunikaciju. Besplatna verzija omogućuje pristup povijesti zadnjih 10.000 timskih poruka, video pozive s kolegama i integrira se s 10 aplikacija. <https://slack.com/> * **Trello**. Ovaj alat je temeljen na Kanban karticama i omogućuje da uključite bilješke, datoteke, rokove i druge stavke. Besplatan je za do 10 ploča po timu. <https://trello.com/>   **Dio 3: Preporuke za poduzetnike i zaposlenike**  **Odjeljak 3.1: Preporuke za poduzetnike**   * Pobrinite se da vaše poduzeće ima **plan kibernetičke sigurnosti** koji odgovara potrebama i potencijalnim ranjivostima vašeg poslovanja. * Uspostavite politike i procedure za **sigurno upravljanje informacijama**, npr. zabranjeno korištenje privatnih uređaja, uništavanje dokumenata na siguran način. * **Informirajte svoje zaposlenike o kibernetičkoj sigurnosti** kako bi se mogli pridržavati pravila i procedura. * **Unaprijedite svoje digitalne i kibersigurnosne vještine**; zapamtite da rukujete vrlo osjetljivim informacijama. * **Pridržavajte se preporuka za zaposlenike!** ☺   **Odjeljak 3.2: Preporuke za zaposlenike**   * Kibernetička sigurnost počinje **fizičkom sigurnošću informacija**: neka vaša radna površina bude čista od povjerljivih informacija, papirića s lozinkama, e-pošte itd. * Ne spajajte **USB uređaje** koji dolaze od nepouzdanih osoba jer bi mogli zaraziti vaše računalo. * **Šifrirajte osjetljive informacije prije slanja**, npr. putem komprimirane datoteke zaštićene lozinkom. * Ne zaboravite **redovito prazniti smeće računala**. * Redovito pravite **sigurnosne kopije**. * Izvan radnog mjesta, **pazite na svoje mobilne uređaje.** * Ako je moguće, **izbjegavajte povezivanje s otvorenim wifi mrežama**. Ako to trebate učiniti, koristite VPN radi sigurnosti. * **Zaključajte svoje računalo** kada niste za radnim stolom. * **Koristite sigurne lozinke**. Možete provjeriti sigurnost svojih lozinki na namjenskim web stranicama za provjeru lozinku kao što je <https://password.kaspersky.com/>. * **Nemojte uvijek koristiti iste lozinke** jer ćete biti ranjiviji u slučaju da “procure”. * **Ne preuzimajte privitke od nepoznatih pošiljatelja**, budite oprezni sa **sumnjivim porukama** i **prijavite svaki incident** svojim nadređenima. | | |
| **Sadržaj u natuknicama** | | |
| * Kibernetička sigurnost nastala je iz potrebe poduzeća da zaštite svoje računalne sustave od zlonamjernih napada. * Najčešći kibersigurnosni incidenti s kojima se suočavaju europska mikro, mala i srednja poduzeća povezani su s *phishingom*. * Kibernetička sigurnost odgovornost je svih u poduzeću te je potrebno imati plan kibernetičke sigurnosti kojeg se uredno pridržavaju menadžeri, direktori i zaposlenici. * U radu na daljinu kibernetička sigurnost nadopunjuje se korištenjem ICT alata koji omogućuju ispunjavanje pet ciljeva kibernetičke sigurnosti u pristupu informacijama. * Poslodavac mora osigurati da postoji plan kibernetičke sigurnosti i da zaposlenici imaju potrebne vještine koje omogućuju da ga se pridržavaju. * Zaposlenici bi trebali biti posvećeni sigurnom upravljanju informacijama tijekom svog rada. | | |
| **5 unosa u pojmovnik** | | |
| **Kibernetička sigurnost.** Uključuje primjenu alata, tehnologija, politika, kontrola i postupaka u zaštiti ili oporavku mreža, sustava, uređaja i aplikacija od kibernetičkih napadakoji su usmjereni na pristup, uništavanje ili mijenjanje osjetljivih informacija, ometanje tijeka rada ili iznuđivanje novca od organizacija ili pojedinaca.  ***Phishing*.** Korisnik dobiva e-poštu koja ga navodi da izvrši neku radnju na lažnoj web stranici, da npr. upiše svoju lozinku ili preuzme zaraženu datoteku. Osim *phishinga* postoje i *vishing* (*voice* + *phishing*) i *smishing* (SMS + *phishing*).  ***Malware*.** *Malware* je zlonamjerni softver koji može imati različite oblike (kod, skripta itd.) i može izvoditi radnje kao što su šifriranje ili brisanje osjetljivih podataka, mijenjanje osnovnih funkcija uređaja, špijuniranje aktivnosti korisnika itd. Računalni virusi, crvi, trojanci, *adware*, *spyware* i *ransomware* također spadaju u *malware*.  **Sigurnosna kopija.** Kopija datoteka i programa koja je pohranjena na drugim uređajima ili drugim medijima, koja omogućava povrat informacija u slučaju kvara, gubitka ili krađe..  **Osjetljive informacije.** Informacije koje sadrže privatne ili povjerljive podatke, poput osobnih ili bankovnih podataka. | | |
| **Bibliografija i daljnje reference** | | |
| <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> | | |
| **Pet pitanja za samoprocjenu s višestrukim izborom**  Nakon završetka procjene sa 75% točnih odgovora, korisnici će moći generirati prilagođenu potvrdu opohađanju i potvrdu o završetku | | **Pitanje 1. Što podrazumijeva "kibernetička sigurnost"?** Opcija a: Alate za zaštitu uređaja od *malware* napada. Opcija b: Postupke koji su osmišljeni kako bi se zaštitile osjetljive informacije od zlonamjernih napada. Opcija c: Zaštitu IT sustava poduzeća. Opcija d: Svi odgovori su točni. **Točan odgovor: d**  **Pitanje 2. Što trebate učiniti da spriječite *phishing*?**  Opcija a: Biti oprezan s neželjenim porukama e-pošte za promjenu lozinke.  Opcija b: Kliknuti na poveznice u e-pošti.  Opcija c: Preuzeti privitke neželjene e-pošte.  Opcija d: Primiti poziv s nepoznatih brojeva.  **Točan odgovor: a**  **Pitanje 3. Koji je najčešći napad na europske MSMEs?**  Opcija a: Uskraćivanje usluge.  Opcija b: *Ransomware*.  Opcija c: *Phishing*.  Opcija d: Ni jedan odgovor nije točan.  **Točan odgovor: c**  **Pitanje 4. Koji su ciljevi kibernetičke sigurnosti za daljinski pristup informacijama?**  Opcija a: Dostupnost, povjerljivost.  Opcija b: Sljedivost, publicitet.  Opcija c: Povjerljivost, korupcija.  Opcija d: Cjelovitost, mjerljivost.  **Točan odgovor: a**  **Pitanje 5. Što učiniti s USB uređajem koji nađete na uredskom stolu?**  Opcija a: Povezati ga s mojim računalom da vidim što je na njemu da ga mogu vratiti vlasniku. Opcija b: Pokušati pronaći vlasnika bez spajanja na bilo koje računalo. Opcija c: Prijavit policiji. Opcija d: Baciti ga. **Točan odgovor: b** |
| **Povezani materijali** | | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_HR.pptx |
| **Povezani linkovi** | | - |
| **Video u YouTube formatu (neobavezno)** | | <https://www.youtube.com/watch?v=PSrnvEEDpuY> |