**Training Fiche**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Naslov** | Varujte svoje podatke: Kibernetska varnost za MSP | | | |
| **Ključne besede** | Kibernetska varnost, Kibernetska varnost, Varovanje podatkov, Varovanje podatkov, Informacijska varnost, Kibernetske grožnje, Vdori podatkov, Varnost omrežij, Upravljanje tveganja, Najboljše prakse na področju varnosti, Kibernetska ozaveščenost | | | |
| **Pripravil** | IT Solutions for All | | | |
| **Jezik** | Slovenščina | | | |
| **Področje usposabljanja** | **☐ Osnove digitalnega podjetništva v okolju mikropodjetij**  **☐ Digitalno komuniciranje in oblikovanje blagovnih znamk**  **☐ Digitalno financiranje**  **☒ kibernetska varnost** | | | |
| **Učni izzid** | **EntreComp** | | | |
| ☐ Ideje in priložnosti  ☒ Viri  ☒ V akcijo  **Obravnavane posebne kompetence:**  Mobilizacija virov, mobilizacija drugih, načrtovanje in upravljanje, spoprijemanje z negotovostjo, dvoumnostjo in tveganjem, učenje z izkušnjami | | | |
| **DigComp** | | | |
| ☐ Informacijska in podatkovna pismenost  ☐ Komunikacija in sodelovanje  ☐ ustvarjanje digitalnih vsebin  ☒ Varnost  ☒ Reševanje problemov  **Posebne obravnavane kompetence:**  Varovanje naprav, varovanje osebnih podatkov in zasebnosti, prepoznavanje potreb in tehnoloških odzivov | | | |
| **Proficiency level** | | | |
| ☐ Level 1  ☐ Level 2 | ☐ Level 3  ☐ Level 4 | ☒ Level 5  ☐ Level 6 | ☐ Level 7  ☐ Level 8 |
| **Foundation** | **Intermediate** | **Advanced** | **Expert** |
| **Opis** | V današnji digitalni dobi so podatki dragoceno premoženje vsake organizacije, tudi mikro, malih in srednjih podjetij (MSME). Vendar pa je z vse večjo odvisnostjo od tehnologije tveganje kibernetskih groženj in kršitev varnosti podatkov še nikoli tako veliko.  Naš tečaj usposabljanja "Varujte svoje podatke: Kibernetska varnost za mala in srednje velika podjetja" je posebej zasnovano tako, da lastnikom, vodjem in zaposlenim v malih in srednje velikih podjetjih omogoči pridobivanje znanja in spretnosti, potrebnih za zaščito njihovih dragocenih podatkov in občutljivih informacij. | | | |
| **Učni cilji** | * celovito razumevanje groženj kibernetske varnosti in potrebnih ukrepov za zaščito svojih MSP. * pridobiti znanje in spretnosti za vzpostavitev varne infrastrukture IT. * da bodo znali upravljati informacijsko varnost in se učinkovito odzvati na incidente s področja kibernetske varnosti. | | | |
| **Kazalo**  **(3 levels: Module-Unit-Section)** | **Modul: Varujte svoje podatke: Kibernetska varnost za mala in srednje velika podjetja**  **Enota 1: Uvod v kibernetsko varnost za MSP**  Razdelek 1.1. Razumevanje kibernetske varnosti: opredelitev in pomen varnostnih politik  Razdelek 1.2. Pogoste grožnje kibernetski varnosti, s katerimi se soočajo MSP  **Enota 2: Vzpostavitev varne infrastrukture IKT**  Razdelek 2.1. Ocenjevanje ranljivosti kibernetske varnosti  Razdelek 2.2. Učinkovita uporaba protivirusnih rešitev in rešitev proti škodljivi programski opremi  **Enota 3: Upravljanje informacijske varnosti**  Razdelek 3.1. Prakse in smernice | | | |
| **Vsebina** | **Modul: Varujte svoje podatke: Kibernetska varnost za mala in srednje velika podjetja**  **Enota 1:** Uvod v kibernetsko varnost za MSP  **Razdelek 1.1.** Razumevanje kibernetske varnosti: opredelitev in pomen varnostnih politik  Varnostna politika za mikro, mala in srednje velika podjetja (MSME) je uradni dokument, ki opisuje pristop organizacije k informacijski varnosti. Določa pravila, smernice in odgovornosti za zaščito sredstev, podatkov in sistemov podjetja pred morebitnimi grožnjami in nepooblaščenim dostopom. Politika mora biti celovita, jasna in prilagojena posebnim potrebam in tveganjem, s katerimi se sooča MMSE. Razumevanje kibernetske varnosti in pomena varnostnih politik za mikro in mala srednja podjetja po COVID je ključno iz več razlogov:  **Zavedanje o kibernetskih grožnjah:** Razumevanje kibernetske varnosti posameznikom omogoča, da se zavedajo različnih kibernetskih groženj in tveganj, ki obstajajo v digitalnem okolju. Pomaga jim prepoznati morebitne ranljivosti in slabosti v njihovih sistemih, omrežjih in praksah.  **Zaščita občutljivih podatkov:** Ukrepi kibernetske varnosti varujejo občutljive in zaupne podatke pred nepooblaščenim dostopom, krajo ali zlorabo. To je še posebej pomembno za mala in srednje velika podjetja, saj pogosto upravljajo z dragocenimi informacijami o strankah, finančnimi podatki in intelektualno lastnino.  **Preprečevanje kršitev podatkov:** Varnostne politike imajo pomembno vlogo pri preprečevanju kršitev varnosti podatkov in kibernetskih napadov. V njih so opisani postopki in smernice, ki zagotavljajo varno ravnanje s podatki in zmanjšanje morebitnih vstopnih točk za napadalce.  **Ohranjanje neprekinjenega poslovanja:** Kibernetska varnost je bistvenega pomena za nemoteno delovanje MSP. Varnostne politike pomagajo pri prepoznavanju morebitnih tveganj, ki bi lahko motila poslovanje, in pomagajo pri razvoju strategij za ohranjanje neprekinjenega poslovanja ob kibernetskih incidentih.  **Skladnost in pravne zahteve:** Številne panoge imajo posebne predpise in pravne zahteve v zvezi z varstvom podatkov in kibernetsko varnostjo. Razumevanje kibernetske varnosti pomaga MSP upoštevati te predpise, se izogniti kaznim ter ohraniti zaupanje strank in partnerjev.  **Krepitev zaupanja strank:** Prikaz zavezanosti kibernetski varnosti in uvedba zanesljivih varnostnih politik lahko povečata zaupanje strank in zaupanje v MMSE. Stranke bodo bolj verjetno poslovale z organizacijami, ki dajejo prednost zaščiti njihovih podatkov in zasebnosti.  **Preprečevanje finančne izgube:** kibernetski napadi lahko povzročijo veliko finančno izgubo za MSP. Razumevanje kibernetske varnosti in izvajanje učinkovitih varnostnih politik lahko pomagata zmanjšati finančna tveganja, povezana s kršitvami varnosti podatkov in drugimi kibernetskimi incidenti.  **Upravljanje ugleda:** Uspešen kibernetski napad lahko škoduje ugledu MSP, kar vodi v izgubo strank in priložnosti. Varnostne politike pomagajo preprečevati incidente in dokazujejo predanost organizacije varovanju informacij.  **Pripravljenost na krize:** Ozaveščenost o kibernetski varnosti in varnostne politike pomagajo MSP, da se pripravijo na morebitne krize in skrajšajo čas obnove.  **Usposabljanje in ozaveščanje zaposlenih:** Razumevanje kibernetske varnosti organizacijam omogoča, da svojim zaposlenim zagotovijo ustrezno usposabljanje. Izobraževanje zaposlenih o najboljših praksah, morebitnih grožnjah in varnostnih politikah pomaga ustvariti močno varnostno kulturo v organizaciji.  **Konkurenčna prednost:** Poudarjanje kibernetske varnosti in vzpostavitev učinkovitih varnostnih politik lahko MSP zagotovi konkurenčno prednost. Stranke in partnerji pri izbiri poslovnih partnerjev pogosto dajejo prednost varnosti, zato je kibernetska varnost dragocen razlikovalni dejavnik.  Zaključimo lahko, da je razumevanje kibernetske varnosti in pomena varnostnih politik temeljnega pomena za MSP, da lahko zaščitijo svoje podatke, ohranijo neprekinjeno poslovanje, spoštujejo predpise ter gradijo zaupanje pri strankah in deležnikih. S proaktivnim obravnavanjem kibernetskih groženj lahko MSP okrepijo svojo odpornost in zagotovijo varno digitalno okolje za svoje delovanje.  **Oddelek 1.2. Pogoste grožnje kibernetski varnosti, s katerimi se soočajo MSP**  Mikro, mala in srednje velika podjetja (MSME) zaradi dragocenih podatkov in potencialno šibkejše kibernetske varnostne zaščite v primerjavi z večjimi organizacijami vse pogosteje postajajo tarče kibernetskih kriminalcev. Nekatere pogoste grožnje kibernetski varnosti, s katerimi se soočajo mala in srednje velika podjetja, vključujejo:  **Napadi ribarjenja:** Pri tem kibernetski kriminalci pošiljajo zavajajoča e-poštna sporočila, sporočila ali spletna mesta, da bi zaposlene prepričali, da razkrijejo občutljive informacije, kot so prijavni podatki, finančni podatki ali osebne informacije.  **Ransomware:** Izkupiček je vrsta zlonamerne programske opreme, ki šifrira podatke organizacije in jih naredi nedostopne, dokler se ne plača odkupnina. MMSP so lahko tarča zaradi domnevno šibkejših varnostnih ukrepov.  **Okužbe s škodljivo programsko opremo:** MMSE so dovzetne za različne vrste zlonamerne programske opreme, vključno z virusi, trojanskimi konji in vohunsko programsko opremo. Ti zlonamerni programi lahko motijo delovanje, ukradejo podatke ali pridobijo nepooblaščen dostop do sistemov.  **Grožnje z notranjimi informacijami:** Z notranjimi grožnjami so povezana zlonamerna dejanja ali nenamerne napake zaposlenih ali posameznikov, ki imajo dostop do sistemov, podatkov ali omrežij organizacije.  **Napadi s socialnim inženiringom:** Socialni inženiring vključuje manipulacijo posameznikov, da razkrijejo zaupne informacije, kot so gesla ali prijavni podatki. To se lahko zgodi s telefonskimi klici, osebnimi stiki ali družabnimi mediji.  **Nezavarovane naprave IoT:** Veliko MSP uporablja naprave interneta stvari (IoT), kot so pametne kamere ali senzorji. Če te naprave niso ustrezno zaščitene, lahko postanejo vstopne točke za vdor napadalcev v omrežje.  **Šibka gesla in preverjanje pristnosti:** Zaradi neustreznih praks glede gesel, kot je uporaba gesel, ki jih je mogoče zlahka uganiti, ali njihova ponovna uporaba v več računih, so lahko MSP ranljiva za napade z grobo silo ali polnjenje poverilnic.  **Vdori podatkov:** MMSP pogosto zbirajo in hranijo dragocene podatke o strankah. Če podatki niso ustrezno zaščiteni, lahko kršitev varstva podatkov povzroči škodo ugledu, finančno izgubo in pravne posledice.  **Napadi z zavrnitvijo storitve (DoS):** Napadi DoS preobremenijo sisteme ali omrežje organizacije s poplavo prometa ter povzročijo motnje in izpade.  **Pomanjkanje rednih posodobitev in popravkov programske opreme:** Če MSP ne uporabljajo pravočasnih posodobitev in varnostnih popravkov za programsko opremo in operacijske sisteme, so lahko izpostavljena znanim ranljivostim.  **Varnostni pomisleki v oblaku:** Shranjevanje podatkov in aplikacij v oblaku je lahko za MSP priročno, vendar lahko povzroči tudi varnostna tveganja, če niso ustrezno konfigurirani in upravljani.  **Napadi na dobavno verigo:** Kibernetski kriminalci lahko z izkoriščanjem ranljivosti v dobavni verigi napadejo MOME kot sredstvo za dostop do večjih organizacij.  **Napačno konfigurirane varnostne nastavitve:** Nepravilno konfigurirane varnostne nastavitve v sistemih, aplikacijah ali omrežnih napravah lahko povzročijo nenamerne varnostne vrzeli.  Pomanjkanje ozaveščenosti zaposlenih o kibernetski varnosti: Nezadostna ozaveščenost in usposabljanje zaposlenih o kibernetski varnosti lahko povečata verjetnost, da postanejo žrtve različnih kibernetskih groženj.  **Enota 2: Vzpostavitev varne infrastrukture IKT**  **Razdelek 2.1.** Ocenjevanje ranljivosti kibernetske varnosti  Ocenjevanje ranljivosti kibernetske varnosti je za MSP bistvenega pomena, saj omogoča ugotavljanje morebitnih pomanjkljivosti njihovih sistemov, infrastrukture IKT, omrežij in praks. V nadaljevanju so predstavljeni koraki, ki jih lahko MMSP izvede za oceno svojih ranljivosti na področju kibernetske varnosti:  **Prepoznajte sredstva in podatke:** Začnite z identifikacijo vseh sredstev, infrastrukture IKT, sistemov, naprav in podatkov, ki jih vaše MMSE uporablja ali hrani. To vključuje strojno in programsko opremo, strežnike, omrežne naprave, storitve v oblaku in občutljive podatke.  **Izvedite oceno tveganja:** Izvedite celovito oceno tveganja, da ugotovite morebitne grožnje, ranljivosti in potencialni vpliv kibernetskega incidenta na vašo organizacijo. Ta ocena vam bo pomagala določiti prednostne naloge za prvo obravnavo najbolj kritičnih tveganj.  **Testiranje prodora:** Razmislite o izvedbi penetracijskega testiranja (etično hekanje) za simulacijo resničnih kibernetskih napadov na vaše sisteme in omrežja. S tem boste lažje ugotovili morebitne vstopne točke in šibka področja v vaši varnostni zaščiti.  **Pregled varnosti omrežja:** Ocenite varnost omrežne infrastrukture, vključno s požarnimi zidovi, usmerjevalniki, stikali in brezžičnimi omrežji. Prepričajte se, da so te naprave ustrezno konfigurirane in da je vzpostavljen nadzor dostopa.  **Ocenite programsko opremo in aplikacije:** Redno preverjajte varnostne posodobitve in popravke za vso programsko opremo in aplikacije, ki jih uporabljate v organizaciji. Zastarela programska oprema lahko ustvari ranljivosti, ki jih lahko izkoristijo kibernetski napadalci.  **Ocenite varnost končnih točk:** Ocenite varnostne ukrepe na končnih napravah (npr. prenosnih računalnikih, pametnih telefonih, tabličnih računalnikih), ki jih uporabljajo zaposleni. Uvedite protivirusno programsko opremo, šifriranje in uveljavite pravila za dostop do podatkov podjetja v osebnih napravah.  **Preverite fizično varnost:** Ne spreglejte fizične varnosti. Ocenite nadzor fizičnega dostopa do pisarniških prostorov, strežniških sob in občutljivih območij, kjer so shranjeni podatki in oprema.  **Preučite ozaveščenost zaposlenih:** Ocenite raven ozaveščenosti zaposlenih o kibernetski varnosti. Izvedite usposabljanje in delavnice, da jih poučite o običajnih kibernetskih grožnjah in najboljših praksah za varnost podatkov.  **Preglejte pravila o geslih:** Zagotovite, da so vzpostavljene stroge politike gesel, vključno z zahtevo po kompleksnih geslih, rednim menjavanjem gesel in prepovedjo ponovne uporabe gesel v več računih.  **Zagotovite storitve v oblaku:** Če uporabljate storitve v oblaku, ocenite njihove varnostne funkcije in zagotovite, da izpolnjujejo zahteve vaše organizacije. Za občutljive podatke, shranjene v oblaku, izvajajte večfaktorsko preverjanje pristnosti in šifriranje.  **Analizirajte varnostne politike:** Redno pregledujte in posodabljajte varnostne politike. Prepričajte se, da so usklajene z industrijskimi standardi in zahtevami glede skladnosti. Te politike morajo zajemati področja, kot so varstvo podatkov, nadzor dostopa, odzivanje na incidente in sprejemljiva uporaba.  **Revizija prodajalcev tretjih oseb:** Če sodelujete s tretjimi prodajalci ali ponudniki storitev, ocenite njihove prakse kibernetske varnosti in ukrepe za zaščito podatkov, da zagotovite, da ne prinašajo dodatnih tveganj.  **Pripravljenost na odzivanje na incidente:** Ocenite načrt odzivanja na incidente v organizaciji in se prepričajte, da je celovit in da zajema ustrezne ukrepe, ki jih je treba sprejeti v primeru kibernetskega incidenta.  **Redne varnostne revizije:** Izvajajte redne varnostne revizije in ocene, da bi ohranili stalno razumevanje položaja kibernetske varnosti vaše organizacije.  **Zagotavljanje varnosti omrežja wi-fi:** Zagotavljanje varnosti omrežij Wi-Fi je ključnega pomena za preprečevanje nepooblaščenega dostopa in zaščito občutljivih podatkov.  To je mogoče doseči z:  ● s spreminjanjem privzetih poverilnic  ● z uporabo močnega šifriranja  ● omogočanjem zaščitenega dostopa wi-fi 3 (WPA3) ali WPA2 s standardom AES (advanced encryption standard) za močno šifriranje  ● izogibanje uporabi zastarelih in ranljivih metod šifriranja, kot je WEP (wired equivalent privacy)  ● sprememba privzetega identifikatorja nabora storitev (SSID) v edinstveno ime, ki ne razkriva informacij o vašem podjetju ali organizaciji  ● izklop oddajanja SSID, da bo vaše omrežje manj vidno morebitnim napadalcem  ● vzpostavitev ločenega omrežja za goste za obiskovalce ali stranke, ki jih izolira od glavnega notranjega omrežja, z uporabo močnih gesel  ● omogočite filtriranje naslovov mac, da se v omrežje wi-fi lahko povežejo samo določene naprave z vnaprej odobrenimi naslovi mac  ● posodabljanje vdelane programske opreme  ● onemogočite oddaljeno upravljanje na usmerjevalniku, da preprečite nepooblaščen dostop zunaj vašega omrežja  ● omogočanje požarnega zidu in šifriranja omrežja  ● onemogočanje univerzalnega priključka in predvajanja (UPNP) na usmerjevalniku, saj ga lahko napadalci izkoristijo za odpiranje vrat in izpostavijo vaše omrežje morebitnim grožnjam  ● spremljanje dejavnosti v omrežju  ● zavarovanje fizičnega dostopa  ● izobraževanje zaposlenih.  **Razdelek 2.2.** Učinkovita uporaba protivirusnih rešitev in rešitev proti škodljivi programski opremi:  Učinkovita uporaba protivirusnih rešitev in rešitev proti škodljivi programski opremi je za mikro, mala in srednje velika podjetja (MSME) ključnega pomena za zaščito njihove infrastrukture IKT, sistemov, omrežij in podatkov pred različnimi kibernetskimi grožnjami.  Tukaj je nekaj najboljših praks za učinkovito uporabo protivirusnih in protivohunskih rešitev:  **Izberite celovito rešitev:** Izberite ugledno in celovito protivirusno in protivohunsko programsko opremo, ki ponuja zaščito v realnem času, redne posodobitve in pogoste preglede za odkrivanje in odstranjevanje zlonamerne programske opreme**.**  **Posodabljajte programsko opremo:** Poskrbite, da bo protivirusna in protivohunska programska oprema posodobljena z najnovejšimi opredelitvami virusov in posodobitvami podatkovne zbirke. To je bistveno za odkrivanje in zaščito pred novimi in nastajajočimi grožnjami.  **Omogočite pregledovanje v realnem času:** V protivirusni programski opremi aktivirajte funkcije pregledovanja v realnem času, da samodejno preverite datoteke, prenose in e-poštne priponke glede zlonamerne programske opreme, ko do njih dostopate.  **Načrtujte redna pregledovanja**: Nastavite načrtovano pregledovanje, ki se izvaja ob primernem času, ko je najmanj verjetno, da bo sistem v intenzivni uporabi, na primer zunaj delovnega časa.  **Omogočite samodejne posodobitve:** Omogočite samodejne posodobitve za protivirusno programsko opremo in operacijski sistem, da zagotovite stalno zaščito pred najnovejšimi grožnjami.  **Izvajajte celotne preglede sistema:** Redno izvajajte celotne preglede sistema, da temeljito preverite vse datoteke, tudi tiste na manj pogosto dostopnih območjih.  **Karantena in izolacija groženj:** Nastavite protivirusno programsko opremo tako, da zaznane grožnje postavi v karanteno ali jih izolira in jim tako prepreči širjenje ali povzročanje nadaljnje škode.  **Preglejte zunanje naprave:** Pred dostopom do datotek preglejte vse zunanje naprave, kot so pogoni USB ali zunanji trdi diski, da preprečite vnos zlonamerne programske opreme v omrežje.  **Izobraževanje zaposlenih:** Izobražujte zaposlene o pomenu protivirusne in protivohunske zaščite ter jih poučite o previdnosti pri priponkah, prenosih in povezavah v e-pošti, da ne bi nenamerno vnesli zlonamerne programske opreme.  **Izvajanje zaščite končne točke:** Razmislite o uporabi rešitev za zaščito končnih točk, ki zagotavljajo večplastno zaščito pred različnimi vrstami groženj, vključno z izsiljevalsko programsko opremo (ransomware) in izkoriščevalskimi napadi ničelnega dne.  **Centralizirano upravljanje**: Če upravljate več sistemov, uporabite centralizirana orodja za upravljanje, da z enega vmesnika spremljate in nadzorujete protivirusno in protimalvarno programsko opremo v vseh napravah.  **Redno vzdrževanje sistema:** Redno izvajajte naloge vzdrževanja sistema, kot sta čiščenje diska in defragmentacija, da optimizirate delovanje sistema in izboljšate učinkovitost protivirusnih pregledov.  **Spremljanje in odzivanje na opozorila:** Nastavite protivirusno programsko opremo za pošiljanje opozoril o zaznanih grožnjah ter se nemudoma odzovite na vsa opozorila in jih raziščite ter ustrezno ukrepajte.  **Občasne varnostne ocene**: Izvajajte redne varnostne ocene in revizije, da ocenite učinkovitost protivirusnih rešitev in rešitev proti škodljivi programski opremi ter opredelite področja za izboljšave.  **Strategije varnostnega kopiranja in obnovitve podatkov:** Izvedite strategijo rednega varnostnega kopiranja podatkov, da zagotovite varnost pomembnih datotek v primeru hude okužbe z zlonamerno programsko opremo ali napada z izsiljevalsko programsko opremo. Vzpostavite redni urnik varnostnega kopiranja, da zagotovite redno varnostno kopiranje ključnih podatkov. Glede na količino podatkov in pogostost sprememb so lahko primerne dnevne, tedenske ali mesečne varnostne kopije. Poleg tega lahko MMSP uporabljajo avtomatizirane rešitve za varnostno kopiranje, da zmanjšajo tveganje človeških napak in zagotovijo, da se varnostne kopije dosledno izvajajo brez ročnega posredovanja. Ne pozabite shraniti varnostnih kopij podatkov na več fizičnih lokacijah, da zmanjšate tveganje izgube podatkov zaradi kraje, požara ali drugih nesreč, ki prizadenejo eno samo lokacijo. Kot stroškovno učinkovito in zanesljivo rešitev poleg varnostnih kopij na lokaciji razmislite tudi o varnostnih kopijah v oblaku. Varnostne kopije v oblaku zagotavljajo enostavno razširljivost, dostopnost in redundanco podatkov.  Ne pozabite, da je kibernetska varnost stalen proces. Redno ocenjevanje, stalno spremljanje in takojšnje ukrepanje za odpravo ranljivosti so bistvenega pomena za zaščito vašega MSP pred razvijajočimi se kibernetskimi grožnjami.  **Enota 3: Upravljanje informacijske varnosti**  **Razdelek 3.1.** Prakse in smernice  Upravljanje varnosti informacij je ključnega pomena za mikro, mala in srednja podjetja (MSME), da **zaščitijo svoje občutljive podatke, ohranijo zaupanje strank** in zaščitijo svoje poslovanje.  Tukaj je nekaj ključnih smernic in praks, ki jih lahko MSME upoštevajo za učinkovito upravljanje informacijske varnosti:  **Ocena tveganja:** Izvedite temeljito oceno tveganja, da prepoznate morebitne ranljivosti in grožnje varnosti informacij. Razumeti vrste podatkov, s katerimi upravlja organizacija, tveganja, povezana z vsako vrsto, in vpliv kršitve varnosti.  **Varnostne politike in postopki:** Razvijte in izvajajte celovite politike in postopke varnosti informacij, ki pokrivajo področja, kot so ravnanje s podatki, nadzor dostopa, upravljanje gesel, varnostno kopiranje podatkov in odziv na incidente.  **Usposabljanje zaposlenih:** Usposobite vse zaposlene o najboljših praksah informacijske varnosti, protokolih za zaščito podatkov in o tem, kako prepoznati varnostne grožnje in se nanje odzvati, kot so napadi lažnega predstavljanja. Izobraževanje zaposlenih o kibernetski varnosti je bistvenega pomena za celovito obrambno strategijo. Napadi družbenega inženiringa in lažno predstavljanje so pogoste grožnje, ki ciljajo na mala in srednja podjetja, zato morajo biti zaposleni sposobni prepoznati in ublažiti njihova tveganja s prepoznavanjem lažnih e-poštnih sporočil, obravnavanjem sumljivih prilog in izvajanjem protokolov za preverjanje pristnosti e-pošte. V tem smislu ima varnost gesel ključno vlogo pri zaščiti občutljivih podatkov. Zaposleni se morajo zavedati praks za ustvarjanje močnih gesel, implementacijo večfaktorske avtentikacije (MFA) in upravljanje politik gesel v organizaciji.  **Nadzor dostopa:** Izvedite nadzor dostopa, da zagotovite, da ima samo pooblaščeno osebje dostop do občutljivih podatkov. Uporabite nadzor dostopa na podlagi vlog, da omejite dostop na podlagi delovnih vlog in odgovornosti.  **Varno ravnanje s podatki:** Vzpostavite smernice za varno ravnanje s podatki, tako v digitalni kot fizični obliki. To vključuje ustrezno shranjevanje, šifriranje in varno odstranjevanje občutljivih informacij.  **Redne posodobitve programske opreme in popravki:** Posodabljajte vso programsko opremo, vključno z operacijskimi sistemi, aplikacijami in varnostnimi orodji, z najnovejšimi popravki in posodobitvami za odpravljanje znanih ranljivosti.  **Požarni zidovi in protivirusna programska oprema:** namestite požarne zidove in ugledno protivirusno/protivirusno programsko opremo za zaščito pred zunanjimi grožnjami.  **Varna konfiguracija omrežja:** varno konfigurirajte omrežja, vključno z omrežji Wi-Fi, da preprečite nepooblaščen dostop in prestrezanje podatkov.  **Varnostno kopiranje in obnovitev podatkov:** redno varnostno kopirajte kritične podatke in testirajte postopek obnavljanja podatkov, da zagotovite neprekinjeno poslovanje v primeru izgube podatkov ali kibernetskega napada.  **Načrt odzivanja na incidente:** Razvijte jasen načrt odzivanja na incidente, ki opisuje korake, ki jih je treba sprejeti v primeru kršitve varnosti ali kršitve podatkov. Dodelite vloge in odgovornosti ključnemu osebju za učinkovito upravljanje incidentov. Priprave na incidente kibernetske varnosti in učinkovito odzivanje nanje so bistvenega pomena za zmanjšanje škode in ublažitev tveganj.  **Upravljanje prodajalca:** če MSME uporablja tretje osebe prodajalce ali ponudnike storitev, opravite potrebno skrbnost, da zagotovite, da so njihove prakse varovanja informacij usklajene s standardi vaše organizacije.  **Nenehno spremljanje in revizija:** izvajajte stalno spremljanje in občasne varnostne revizije za proaktivno odkrivanje in reševanje morebitnih varnostnih težav.  **Skladnost s predpisi o zasebnosti podatkov:** Bodite na tekočem z ustreznimi zakoni in predpisi o zasebnosti podatkov, ki veljajo za poslovanje MSME. Upoštevajte zahteve glede varstva podatkov in obveščajte stranke o praksah ravnanja s podatki.  **Varnostna ozaveščenost in kultura:** spodbujajte kulturo varnostne ozaveščenosti in odgovornosti med zaposlenimi. Spodbujajte poročanje o varnostnih incidentih in pomislekih.  **Redni varnostni pregledi:** izvajajte redne varnostne preglede in ocene tveganja, da prepoznate nastajajoče grožnje in potencialna področja za izboljšave.  S proaktivnim upravljanjem informacijske varnosti lahko mala in srednja podjetja zmanjšajo tveganje kršitev podatkov, zaščitijo občutljive informacije in zgradijo zaupanje strank in partnerjev, kar na koncu prispeva k dolgoročnemu uspehu podjetja. | | | |
| **Glosar** | **Internet stvari (IoT**). Internet stvari ali IoT je sistem medsebojno povezanih računalniških naprav, mehanskih in digitalnih strojev, predmetov, živali ali ljudi, ki so opremljeni z edinstvenimi identifikatorji (UID) in zmožnostjo prenosa podatkov po omrežju, ne da bi zahtevali povezavo človek-to- interakcija človek ali človek-računalnik.  Vir: TechTarget <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>  **Zavrnitev storitve (DoS).** Zavrnitev storitve (DoS) je vrsta kibernetskega napada, namenjenega onemogočanju, zaustavitvi ali motnjam v omrežju, spletnem mestu ali storitvi. Običajno se zlonamerna programska oprema uporablja za prekinitev ali zaviranje običajnega pretoka podatkov v sistem in iz njega, da postane tarča za določeno obdobje neuporabna ali nedostopna. Primer napada DoS: ko se do spletnega mesta množično in večkrat dostopa z različnih lokacij, kar zakonitim obiskovalcem prepreči dostop do spletnega mesta.  Vir: Trend Micro <https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos>  **Večfaktorska avtentikacija.** Večfaktorsko preverjanje pristnosti (MFA) je metoda preverjanja pristnosti, ki od uporabnika zahteva, da zagotovi dva ali več dejavnikov preverjanja, da pridobi dostop do vira, kot je aplikacija, spletni račun ali VPN. MFA je osrednja komponenta močne politike upravljanja identitete in dostopa (IAM). Namesto da samo zahteva uporabniško ime in geslo, MFA zahteva enega ali več dodatnih dejavnikov preverjanja, kar zmanjša verjetnost uspešnega kibernetskega napada.  Vir: Onelogin <https://www.onelogin.com/learn/what-is-mfa>  **Identifikator nabora storitev (SSID**). (Service Set IDentifier) Ime, dodeljeno (brezžičnemu) omrežju Wi-Fi. Vse naprave v omrežju morajo za komunikacijo prek omrežja Wi-Fi uporabljati to ime, ki razlikuje med velikimi in malimi črkami, kar je besedilni niz, dolg do 32 bajtov. Brezžični usmerjevalniki in dostopne točke imajo takoj po namestitvi privzeti SSID, ki je lahko ime proizvajalca, na primer »linksys« ali »netgear« ali preprosto »default«. Nekatere naprave uporabljajo svojo številko modela kot SSID. Z uporabo spletnega brskalnika lahko SSID (in geslo) ročno spremenite v konfiguracijskih nastavitvah naprave.  **Vir: PcMag** [**https://www.pcmag.com/encyclopedia/term/ssid**](https://www.pcmag.com/encyclopedia/term/ssid)  **Universal Plug and Play (UPnP).** UPnP (Universal Plug and Play) je omrežni protokol, ki omogoča napravam, da odkrijejo druga drugo in se povežejo brez potrebe po ročni konfiguraciji ali posredovanju uporabnika. Protokol avtomatizira vse korake, potrebne za prepoznavanje in komunikacijo med napravami v istem omrežju.  Vir: **PhoenixNap** <https://phoenixnap.com/blog/what-is-upnp>  **Izkoriščanja ničelnega dne:** Izkoriščanje ničelnega dne (0day) je kibernetski napad, usmerjen v ranljivost programske opreme, ki je prodajalec programske opreme ali prodajalci protivirusnih programov ne poznajo. Napadalec opazi ranljivost programske opreme, preden katera koli stran, ki jo želi ublažiti, hitro ustvari izkoriščanje in ga uporabi za napad. Takšni napadi bodo zelo verjetno uspešni, ker obramba ni vzpostavljena. Zaradi tega so napadi ničelnega dne resna varnostna grožnja.  Vir: **Imperva** <https://www.imperva.com/learn/application-security/zero-day-exploit/>  **Izsiljevalska programska oprema:** izsiljevalska programska oprema je vrsta zlonamerne programske opreme, ki uporabnikom preprečuje ali omejuje dostop do njihovega sistema, tako da zaklene zaslon sistema ali zaklene datoteke uporabnikov, dokler ni plačana odkupnina. Sodobnejše družine izsiljevalskih programov, ki so skupaj kategorizirane kot kripto-izsiljevalci, šifrirajo določene vrste datotek v okuženih sistemih in prisilijo uporabnike, da plačajo odkupnino prek določenih načinov spletnega plačila, da dobijo ključ za dešifriranje.  Vir: **Trend Micro** [**https://www.trendmicro.com/vinfo/us/security/definition/ransomware**](https://www.trendmicro.com/vinfo/us/security/definition/ransomware) | | | |
| **5 izbirnih vprašanj za samoocenjevanje** | **Vprašanje 1. Kaj je varnostna politika?**  Možnost a: Je neuraden dokument, ki opisuje pristop organizacije do  varnost informacij  Možnost b: Je uradni dokument, ki določa pravila, smernice in odgovornosti  za zaščito sredstev, podatkov in sistemov podjetja pred morebitnimi grožnjami in  nepooblaščen dostop  Možnost c: Politika zaščite samo sredstev podjetja  Možnost d: možnosti drevesa so pravilne  **Pravilna možnost: b**  **Vprašanje 2. Zakaj je pomembno razumeti kibernetsko varnost in varnost**  **pravila?**  Možnost a: Razumevanje kibernetske varnosti posameznikom omogoča, da se zavedajo različnih  kibernetske grožnje in tveganja, ki obstajajo v digitalnem okolju  Možnost b: ukrepi kibernetske varnosti ščitijo občutljive in zaupne podatke pred  nepooblaščen dostop, krajo ali zlorabo  Možnost c: varnostne politike igrajo pomembno vlogo pri preprečevanju kršitev podatkov in  kibernetski napadi  Možnost d: Pravilni so trije odgovori  **Pravilna možnost: d**  **Vprašanje 3. Prosimo, označite kateri odgovor je pravilen:**  Možnost a: Kibernetski napadi lahko malim in srednjim podjetjem povzročijo zanemarljive finančne izgube  Možnost b: uspešen kibernetski napad lahko škoduje ugledu MSME, kar povzroči a  izguba strank in priložnosti  Možnost c: izobraževanje osebja o najboljših praksah, potencialnih grožnjah in varnosti politike pomagajo ustvariti močno varnostno kulturo znotraj organizacije  Možnost d: Stranke in partnerji pri izbiri pogosto ne dajejo prednosti varnosti  poslovni partnerji, zaradi česar je kibernetska varnost dragocen diferenciator  **Pravilna možnost: b & c**  **Vprašanje 4. Prosimo, izpostavite pogoste grožnje kibernetski varnosti za MMSP**  Možnost a: Insider poslastice, okužbe in dobro konfigurirane varnostne nastavitve  Možnost b: Vdor podatkov, šibka gesla in preverjanje pristnosti, okužbe z zlonamerno programsko opremo  Možnost c: napadi lažnega predstavljanja, napadi na dobavno verigo, nezavarovane naprave IoT  Možnost d: Vsi odgovori so nepravilni  **Pravilna možnost: b & c**  **Vprašanje 5. Katere korake lahko sprejme MSME za oceno svoje kibernetske varnosti/ranljivosti?**  Možnost a: Preverite fizično varnost, preglejte ozaveščenost zaposlenih in preglejte Politike gesel  Možnost b: Identifikacija sredstev in podatkov, izvedba ocene tveganja in fizični pregled  Varnost  Možnost c: Zagotavljanje varnosti omrežja Wi-Fi, testiranje prodora in ocena  Programska oprema in aplikacije  Možnost d: Pravilni so trije odgovori  **Pravilna možnost: d**  **​** | | | |
| **Bibliografija in drugi viri** | Forbes Tech Council. (2023, May 25). Small But Mighty: Cybersecurity Best Practices for SMEs. Forbes. <https://www.forbes.com/sites/forbestechcouncil/2023/05/25/small-but-mighty-cybersecurity-best-practices-for-smes/?sh=44510c371a33>  Devonshire Green (n.d.). The Importance of Cybersecurity for SMEs. Devonshire Green. <https://www.devonshiregreen.uk/the-importance-of-cybersecurity-for-smes/>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity for SMEs: Challenges and Recommendations. ENISA. <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes/@@download/fullReport>  European Union Agency for Cybersecurity (ENISA). (2021). Cybersecurity Guide for SMEs. ENISA. <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes/@@download/fullReport>  Ministry of Economy and Competitiveness (Spain). (2021). Digitalisation Plan for SMEs [PDF]. Government of Spain. <https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210902-digitalisation-smes-plan.pdf>  Yerik Afrianto Singgalen. (2021, August). Exploring MSMEs' Cybersecurity Awareness and Risk Management: Information Security Awareness. ResearchGate. <https://www.researchgate.net/publication/353622348_Exploring_MSMEs_>  Cybersecurity\_Awareness\_and\_Risk\_Management\_Information\_Security\_Awareness | | | |
| **Povezan material** | DREAM\_WP3\_Cybersecurity\_ITSFA\_EN | | | |
| **Video** | [link] | | | |