AGENCIJA EVROPSKE UNIJE ZA
KIBERNETSKO VARNOST

ECSF

EVROPSKI OKVIR ZNANJA IN SPRETNOSTI NA PODROČJU KIBERNETSKE VARNOSTI

SEPTEMBER 2022

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost ENISA je agencija Unije, ki si prizadeva doseči visoko skupno raven kibernetske varnosti po vsej Evropi. Agencija Evropske unije za kibernetsko varnost, ki je bila ustanovljena leta 2004 in okrepljena z aktom EU o kibernetski varnosti, prispeva k kibernetski politiki EU, povečuje zanesljivost proizvodov, storitev in postopkov IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi pri pripravi na kibernetske izzive prihodnosti. Agencija z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter nazadnje ohranila digitalno varnost evropske družbe in državljanov. Več informacij o agenciji ENISA in njenem delu je na voljo na: www.enisa.europa.eu.

KONTAKT

Za stik z urednikom pišite na euskills@enisa.europa.eu.

PRIZNANJA

Ta okvir je rezultat strokovnega mnenja in dogovora v začasni delovni skupini za okvir znanj in spretnosti, ki jo sestavljajo Agata Bekier, Vladlena BENSON, Jutta BREYER,*Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku Korkiakoski, Csaba Krasznay, Haralambos Mouratidis, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta PolemI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN in Jan Hajny.

Fabio DI FRANCO in Athanasios GRAMMATOPOULOS sta to dejavnost vodila za agencijo ENISA.

PRAVNO OBVESTILO

OBVESTILO O AVTORSKIH PRAVICAH

ISBN: 978–92–9204–584–5 – DOI: 10.2824/859537

KAZALO VSEBINE

1. PREGLED 4
2. PROFILI 5
2.1 VODJA INFORMACIJSKE VARNOSTI (CISO) 5
2.2 UPRAVITELJ V PRIMERU KIBERNETSKIH NAPADOV 7
2.3 POOBLAŠČENEC ZA PRAVNE ZADEVE, POLITIKO IN SKLADNOST V KIBERNETSKEM PROSTORU 9
2.4 STROKOVNJAK ZA KIBERNETSKE GROŽNJE 12
2.5 ARHITEKT KIBERNETSKE VARNOSTI 13
2.6 RAZISKOVALEC KIBERNETSKE VARNOSTI 15
2.7 PREDAVATELJ KIBERNETSKE VARNOSTI 16
2.8 IZVAJALEC KIBERNETSKE VARNOSTI 17
2.9 RAZISKOVALEC KIBERNETSKE VARNOSTI 18
2.10 VODJA TVEGANJ KIBERNETSKE VARNOSTI 19
2.11 PREISKOVALEC DIGITALNE FORENZIKE 20
2.12 IZVAJALEC PENETRACIJSKIH TESTOV 21
3. KNJIŽNICA KONČNIH IZDELKOV 22

1. PREGLED

Vodja informacijske varnosti (CISO)

Upravitelj v primeru kibernetskih napadov

Pooblaščenec za pravne zadeve, politiko in skladnost v kibernetskem

Strokovnjak za kibernetske grožnje

Arhitekt kibernetske varnosti

Revizor kibernetske varnosti

Predavatelj kibernetske varnosti

Izvajalec kibernetske varnosti

Raziskovalec kibernetske varnosti

Vodja tveganj kibernetske varnosti

Preiskovalec digitalne forenzike

Izvajalec penetracijskih testov

2. PROFILI

2.1 VODJA INFORMACIJSKE VARNOSTI (CISO)

Naslov profila	Vodja informacijske varnosti (CISO)
Nadomestni naslov(i)	Direktor programa kibernetske varnosti Uradnik za informacijsko varnost (ISO) Vodja oddelka informacijske varnosti Vodja IT/ IKT varnosti
Povzetek izjave	Upravlja strategijo kibernetske varnosti organizacije in njeno izvajanje, da zagotovi, da zagotovi ustrezno varnost in zaščito digitalnih sistemov, storitev ter sredstev
Misija	Opredeljuje, vzdržuje in sporoča vizijo, strategijo, politike in postopke kibernetske varnosti. Upravlja izvajanje politike kibernetske varnosti v celotni organizaciji. Zagotavlja izmenjavo informacij z zunanjimi organi in strokovnimi telesi.
Končni rezultati	• Strategija za kibernetsko varnost • Politika kibernetske varnosti
Glavna(-a) naloga(-e)	• Opredelitev, izvajanje, sporočanje in vzdrževanje ciljev, zahtev, strategij, politik na področju kibernetske varnosti, usklajenih s poslovno strategijo za podporo organizacijskih ciljev • Pripraviti in predstaviti vizijo, strategije in politike kibernetske varnosti v odobritev višjemu vodstvu organizacije in zagotoviti njihovo izvajanje; • Nadzor nad uporabo in izboljšanjem sistema upravljanja informacijske varnosti (ISMS) • Izobraževati višje vodstvo o tveganjih, grožnjah za kibernetsko varnost in njihovem vplivu na organizacijo • Zagotoviti, da višje vodstvo odobri tveganja za kibernetsko varnost organizacije • Priprava načrtov kibernetske varnosti • Razvoj odnosov z organi in skupnostmi, povezanimi s kibernetsko varnostjo • Poročanje višjemu vodstvu o kibernetskih incidentih, tveganjih in ugotovitvah • Spremljanje napredka na področju kibernetske varnosti • Zagotavljanje virov za izvajanje strategije za kibernetsko varnost • Pogajanja o proračunu za kibernetsko varnost z višjim vodstvom • Zagotavljanje odpornosti organizacije na kibernetske incidente • Vodenje stalne krepitve zmogljivosti v organizaciji • Pregled, načrtovanje in dodeljevanje ustreznih virov za kibernetsko varnost
Ključne spretnosti	• Ocena in izboljšanje položaja organizacije na področju kibernetske varnosti • Analiza in izvajanje politik, certifikatov, standardov, metodologij in okvirov kibernetske varnosti • Analiza in skladnost z zakoni, predpisi in zakonodajami, povezanimi s kibernetsko varnostjo • Izvajanje priporočil in najboljših praks na področju kibernetske varnosti • Upravljanje virov kibernetske varnosti • Razvoj, spodbujanje in vodenje izvajanja strategije za kibernetsko varnost • Vplivanje na kulturo kibernetske varnosti organizacije • Zasnova, uporaba, spremljanje in pregled sistema upravljanja informacijske varnosti (ISMS) bodisi neposredno bodisi z uporabo zunanjega izvajalca. • Pregled in izboljšanje varnostnih dokumentov, poročil in sporazumov o ravni storitve ter zagotavljanje varnostnih ciljev • Opredelitev in reševanje vprašanj, povezanih s kibernetsko varnostjo • Priprava načrta za kibernetsko varnost • Komuniciranje, usklajevanje in sodelovanje z notranjimi in zunanjimi deležniki • Predvidevanje potrebnih sprememb strategije informacijske varnosti organizacije in oblikovanje novih načrtov

	• Opredelitev in uporaba modelov zrelosti za upravljanje kibernetske varnosti • Predvidevanje kibernetskih groženj, potreb in prihodnjih izzivov • Motivirati in spodbujati ljudi	
Ključno znanje	• Politike kibernetske varnosti • Standardi, metodologije in okviri kibernetske varnosti • Priporočila in najboljše prakse na področju kibernetske varnosti • Zakoni, predpisi in zakonodaja, povezani s kibernetsko varnostjo • Certifikati v zvezi s kibernetsko varnostjo • Zahteve glede etičnih organizacij kibernetske varnosti • Modeli zrelosti kibernetske varnosti • Postopki za kibernetsko varnost • Upravljanje virov • Prakse upravljanja • Standardi, metodologije in okviri za obvladovanje tveganj	
e-kompetence (iz e-CF)	A.7. Spremljanje tehnoloških trendov D.1. Razvoj strategije informacijske varnosti E.3. Obvladovanje tveganj E.8. Upravljanje informacijske varnosti E.9. IS-upravljanje	Stopnja 4 Stopnja 5 Stopnja 4 Stopnja 4 Stopnja 5

2.2 UPRAVITELJ V PRIMERU KIBERNETSKIH NAPADOV

Naslov profila	Upravitelj v primeru kibernetskih napadov
Nadomestni naslov(i)	Nadzornik kibernetskih incidentov Strokovnjak za kibernetske krize Inženir za odzivanje na incidente Center za varnostne operacije (SOC) analitik Kibernetski varnostnik Analitik varnostne operacije (SOC analitik) Vodja kibernetske varnosti SIEM
Povzetek izjave	Spremljanje stanja kibernetske varnosti organizacije, obvladovanje incidentov med kibernetskimi napadi in zagotavljanje neprekinjenega delovanja sistemov IKT.
Misija	Spremlja in ocenjuje stanje kibernetske varnosti sistemov. Analizira, ocenjuje in blaži vpliv kibernetskih incidentov. Opredeljuje temeljne vzroke kibernetskih incidentov in zlonamerne akterje. V skladu z načrtom organizacije za odzivanje na incidente ponovno vzpostavi funkcionalnost sistemov in procesov v operativno stanje, zbira dokaze in dokumentira sprejete ukrepe.
Končni rezultati	• Načrt odzivanja na incidente • Poročilo o kibernetskih incidentih
Glavna(-a) naloga(-e)	• Sodelovanje pri razvoju, vzdrževanju in ocenjevanju načrta za odzivanje na incidente • Razvoj, izvajanje in ocenjevanje postopkov v zvezi z obravnavanjem incidentov • Prepoznavanje, analiziranje, ublažitev in sporočanje kibernetskih incidentov • Ocenjevanje in upravljanje tehničnih ranljivosti • Merjenje učinkovitosti odkrivanja in odzivanja kibernetskih incidentov • Ocena odpornosti nadzora kibernetske varnosti in blažilnih ukrepov, sprejetih po incidentu v zvezi s kibernetsko varnostjo ali kršitvijo varnosti podatkov • Sprejemanje in razvoj tehnik testiranja obvladovanja incidentov • Vzpostaviti postopke za analizo rezultatov incidentov in poročanje o incidentih • Dokumentiranje analize rezultatov incidentov in ukrepov za njihovo obvladovanje • Sodelovanje s centri za varno delovanje (SOC) in skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT) • Sodelovanje s ključnim osebjem za poročanje o varnostnih incidentih v skladu z veljavnim pravnim okvirom
Ključne spretnosti	• Izvajanje vseh tehničnih, funkcionalnih in operativnih vidikov obvladovanja kibernetskih incidentov in odzivanja nanje • Zbiranje, analiza in korelacija informacij o kibernetskih grožnjah, ki izvirajo iz več virov • Delo na operacijskih sistemih, strežnikih, oblakih in ustrezni infrastrukturi • Delo pod pritiskom • Obveščanje in predstavitev ustreznih deležnikov ter poročanje o njih • Upravljanje in analiziranje dnevniških datotek
Ključno znanje	• Standardi, metodologije in okviri za obravnavo incidentov • Priporočilo za obravnavo incidentov in najboljše prakse • Orodja za obravnavo incidentov • Komunikacijski postopki obravnavo incidentov • Varnost operacijskih sistemov • Varnost računalniških omrežij • Kibernetske grožnje • Postopki napadov na kibernetsko varnost • Ranljivosti računalniških sistemov • Certifikati v zvezi s kibernetsko varnostjo • Zakoni, predpisi in zakonodaja, povezani s kibernetsko varnostjo • Operacija varnih operativnih centrov (SOC) • Delovanje skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT)
e-kompetence (iz e-CF)	A.7. Spremljanje tehnoloških trendov Stopnja 3 B.2. Vključevanje sestavnih delov Stopnja 2

	B.3. Preizkušanje B.5. Izdelava dokumentacije C.4. Obvladovanje težav	Stopnja 3 Stopnja 3 Stopnja 4

2.3 POOBLAŠČENEC ZA PRAVNE ZADEVE, POLITIKO IN SKLADNOST V KIBERNETSKEM PROSTORU

Naslov profila	Pooblaščenec za pravne zadeve, politiko in skladnost v kibernetskem prostoru
Nadomestni naslov(i)	Pooblaščenec za varstvo podatkov Pooblaščenec za varstvo zasebnosti Svetovalec za kibernetsko pravo Pravni svetovalec za kibernetsko varnost Uradnik za upravljanje informacij Uradnik za skladnost s podatki Pooblaščenec za kibernetsko varnost Vodja skladnosti IT/IKT Svetovalec za upravljanje tveganje in skladnost (GRC)
Povzetek izjave	Skrbi za skladnost s standardi, povezanimi s kibernetsko varnostjo, pravnimi in regulativnimi okviri na podlagi strategije in pravnih zahtev organizacije.
Misija	Nadzoruje in zagotavlja skladnost s pravnimi, regulativnimi okviri in politikami, povezanimi s kibernetsko varnostjo in podatki, v skladu s strategijo in pravnimi zahtevami organizacije. Prispeva k ukrepom, povezanim z varstvom podatkov organizacije. Zagotavlja pravno svetovanje pri razvoju procesov upravljanja kibernetske varnosti v organizaciji in priporoča strategije/rešitve za zagotavljanje skladnosti.
Končni rezultati	• Priročnik o skladnosti • Poročilo o skladnosti
Glavna(-a) naloga(-e)	• Zagotavljanje skladnosti s standardi, zakoni in predpisi o zasebnih podatkih, varstvu podatkov ter pravno svetovanje in smernice področja. • Prepoznavanje in beleženje vrzeli v skladnosti • Izvajanje ocene vpliva na zasebnost ter postopki razvijanja, vzdrževanja, obveščanja in usposabljanja o postopkih politike zasebnosti • Uveljavljanje in promoviranje programa organizacije za varovanje podatkov in varstvo podatkov • Zagotavljanje, da so lastniki, imetniki, upravljavci, pooblaščenci, posamezniki, notranji ali zunanji partnerji in subjekti obveščeni o svojih pravicah, obveznostih in odgovornostih v zvezi z varstvom podatkov; • Delovanje kot ključna kontaktna točka obravnave vprašanj in pritožb glede obdelave podatkov • Pomoč pri oblikovanju, izvajanju, reviziji in preizkušanju skladnosti zagotavljanja kibernetske varnosti in skladnosti z zasebnostjo; • Spremljanje revizij in procesa usposabljanja o varnosti podatkov • Sodelovanje in izmenjava informacij z organi in strokovnimi skupinami • Prispevanje k razvoju strategije, politike in postopkov kibernetske varnost organizacije • Razvoj in predlogi usposabljanja ozaveščanja osebja za doseganje skladnosti in spodbujanje kulture varstva podatkov v organizaciji • Upravljanje pravnih vidikov odgovornosti informacijske varnosti in odnosov s tretjimi osebami
Ključne spretnosti	• Celovito razumevanje poslovne strategije, modelov in produktov ter sposobnost upoštevanja pravnih in regulativnih zahtev ter zahtev standardov • Izvajanje delovnih praks vprašanj varstva podatkov in zasebnosti, povezanih z izvajanjem organizacijskih procesov, financ in poslovne strategije; • Vodenje ustreznih razvojnih politik in postopkov na področju kibernetske varnosti in zasebnosti, ki dopolnjujejo poslovne potrebe in pravne zahteve; nadalje zagotoviti njegovo sprejetje, razumevanje in izvajanje ter obveščanje vseh udeležencev. • Izvajanje, spremljanje in pregled ocen vpliva na zasebnost uporabe standardov, okvirov, priznanih metodologij in orodij • Pojasnjevanje in posredovanje tem o varstvu podatkov in zasebnosti zainteresiranim deležnikom in uporabnikom • Razumevanje, izvajanje in upoštevanje etičnih zahtev in standardov • Razumevanje spremembe pravnega okvira, ki vplivajo na strategijo in politike organizacije na področju kibernetske varnosti in varstva podatkov • Sodelovanje z drugimi člani skupine in sodelavci

Ključno znanje	• Zakoni, predpisi in zakonodaja, povezani s kibernetsko varnostjo • Standardi, metodologije in okviri za kibernetsko varnost • Politike kibernetske varnosti • Zahteve glede pravne, regulativne in zakonodajne skladnosti, priporočila in najboljše prakse Standardi, metodologije in okviri za oceno učinka na zasebnost

e-kompetence (iz e-CF)	A.1. Usklajenost Informacijski sistemi in poslovne strategije D.1. Razvoj strategije informacijske varnosti E.8. Upravljanje informacijske varnosti E.9. IS-upravljanje	Stopnja 4 Stopnja 4 Stopnja 3 Stopnja 4

2.4 STROKOVNJAK ZA KIBERNETSKE GROŽNJE

Naslov profila	Arhitekt kibernetske varnosti
Nadomestni naslov(i)	Analitik kibernetske groženje Oblikovalec modelov kibernetskih groženj
Povzetek izjave	Zbiranje, obdelava, analiza podatkov in informacij za pripravo poročil nevarnostih, ki jih je mogoče izvesti, in njihovo razširjanje ciljnim deležnikom.
Misija	Upravlje življenjskega cikla podatkov o kibernetskih grožnjah, vključno z zbiranjem informacij o kibernetskih grožnjah, analizo in pripravo akcijskih načrtov ter razširjanje informacij varnostnim deležnikom in skupnosti CTI na taktični, operativni in strateški ravni. Opredeljevanje in spremljanje taktike, trendov, tehnik in postopkov, ki jih uporabljajo akterji kibernetskih groženj. Spremlja dejavnosti akterjev groženj ter opazovanje, kako lahko ne kibernetski dogodki vplivajo na dejanja, povezana s kibernetsko varnostjo.
Končni rezultati	• Priročnik o kibernetskih grožnjah • Poročilo o kibernetski grožnji
Glavna(-a) naloga(-e)	• Razvoj, izvajanje in upravljanje strategije organizacije obveščanja o kibernetskih grožnjah • Razvoj načrtov in postopkov za upravljanje podatkov o grožnjah • Pretvorba poslovnih zahtev v varnostne zahteve • Zbiranje podatkov o grožnjah, analiza in priprava podatkov, o mogoči izvedbi napadov, ter razširjanje informacij zainteresiranim stranem na področju varnosti • Opredeljevanje in ocenjevanje akterjev kibernetskih groženj, škodljivih za organizacijo • Opredeljevanje, spremljanje in ocenjevanje taktik, tehnik in postopkov, ki jih uporabljajo akterji kibernetskih groženj, pri čemer uporabljajo analizo prosto dostopnih in zasebnih podatkov in informacij • Priprava poročil sprejetih na podlagi podatkov o kibernetskih grožnjah • Priprava načrtov za blažitev podnebnih sprememb in svetovanje o njihovi implementaciji na taktični, operativni in strateški ravni; • Usklajevanje z deležniki za izmenjavo in uporabo podatkov o kibernetskih grožnjah • Uporaba podatkov za podporo in pomoč pri modeliranju groženj, priporočila za zmanjševanje tveganj in lovu na kibernetske grožnje • Odprto in transparentno sporočanje podatkov o grožnjah na vseh ravneh • Predstavitev varnostnih groženj tako, da se izpostavljenost tveganju in njene posledice pojasnijo tudi ne tehničnim deležnikom
Ključne spretnosti	• Sodelovanje z drugimi člani skupine in sodelavci • Zbiranje, analiza in korelacija informacij o kibernetskih grožnjah iz različnih virov • Prepoznavanje škodljivih akterjev TTP in njihovih aktivnosti • Avtomatizacija postopkov za upravljanje podatkov o grožnjah • Izvajanje tehnične analize in poročanja • Opredelitev dejavnosti ne kibernetskih dogodkov, ki vplivajo na kibernetsko varnost • Modelne grožnje, akterji in TTP-ji • Komuniciranje, usklajevanje in sodelovanje z notranjimi in zunanjimi deležniki • Obveščanje in poročanje relevantnim deležnikom • Uporaba platform in orodij CTI
Ključno znanje	• Varnost operacijskih sistemov • Varnost računalniških omrežij • Upravljanje kibernetske varnosti in rešitve • Računalniško programiranje • Izmenjava standardov, metodologij in okvirov podatkov o kibernetskih grožnjah • Postopki za razkrivanje informacij • Interdisciplinarna znanja povezana s kibernetsko varnostjo • Kibernetske grožnje • Akterji kibernetskih groženj • Postopki napadov na kibernetsko varnost • Napredne in trajne kibernetske grožnje (APT) • Taktike, tehnike in postopki (TTP) akterjev groženj • Certifikati povezani s kibernetsko varnostjo

e-kompetence (iz e-CF)	B.5. Izdelava dokumentacije D.7. Podatkovna znanost in analitika D.10. Upravljanje informacij in znanja E.4. Upravljanje odnosov E.8. Upravljanje informacijske varnosti	Stopnja 3 Stopnja 4 Stopnja 4 Stopnja 3 Stopnja 4

2.5 ARHITEKT KIBERNETSKE VARNOSTI

Naslov profila	Arhitekt za kibernetsko varnost
Nadomestni naslov(i)	Arhitekt rešitev kibernetske varnosti Oblikovalec kibernetske varnosti Arhitekt varnosti podatkov
Povzetek izjave	Načrtuje in oblikuje rešitve za varnost glede na zasnovo (infrastrukture, sistemi, sredstva, programska oprema, strojna oprema in storitve) in kontrole kibernetske varnosti.
Misija	Oblikuje rešitve, ki temeljijo na načelih vgrajene varnosti in vgrajene zasebnosti. Ustvarja in nenehno izboljšuje arhitekturne modele ter razvija ustrezno arhitekturno dokumentacijo in specifikacije. Usklajuje varen razvoj, integracijo in vzdrževanje komponent kibernetske varnosti v skladu s standardi in drugimi povezanimi zahtevami.
Končni rezultati	• Diagram arhitekture kibernetske varnosti • Poročilo o zahtevah kibernetske varnosti
Glavna(-a) naloga(-e)	• Oblikovanje in priporočila varne arhitekture za izvajanje strategije organizacije • Razvoj arhitekture kibernetske varnosti organizacije za obravnavanje zahtev varnosti in zasebnosti • Izdelava arhitekturne dokumentacije in specifikacij • Visokonivojska predstavitev varnostne arhitekture zainteresiranim stranem • Vzpostavitev varnega okolja med razvojnim ciklom sistemov, storitev in izdelkov • Usklajevanje razvoja, povezovanja in vzdrževanja komponent kibernetske varnosti za zagotavljanje varnostnih zahtev kibernetske varnosti • Analiza in ocena kibernetske varnosti arhitekture organizacije • Zagotavljanje varnosti arhitekturnih rešitev z varnostnimi pregledi in certificiranjem • Sodelujte z drugimi ekipami in sodelavci • Ocenjevanje vpliva rešitev kibernetske varnosti na zasnovo in delovanje arhitekture organizacije • Prilagajanje strukture organizacije novim grožnjam • Ocenjevanje arhitekture, za ohranjanje ustrezne ravni varnosti
Ključne spretnosti	• Izvajanje analize uporabniških in poslovnih varnostnih zahtev • Risanje arhitekturnih in funkcionalnih specifikacij kibernetske varnosti • Razčlenitev in analiza sistemov za oblikovanje zahtev razvoj varnosti in zasebnosti ter določitve učinkovitih rešitve • Oblikovalski sistemi in arhitekture, ki temeljijo na vgrajeni varnosti in zasebnosti ter privzetih načelih kibernetske varnosti • Vodi in komunicira z izvajalci in osebjem IT/OT • Obveščanje in predstavitev ustreznih deležnikov ter poročanje o njih • Predlagati arhitekture kibernetske varnosti na podlagi potreb in proračuna deležnikov • Izberite ustrezne specifikacije, postopke in kontrole • Krepitev odpornosti proti točkam neuspeha v arhitekturi • Usklajevanje integracije varnostnih rešitev
Ključno znanje	• Certifikati iz področja kibernetske varnosti • Priporočila in dobre prakse na področju kibernetske varnosti • Standardi, metodologije in okviri kibernetske varnosti • Analiza zahtev kibernetske varnosti • Varen življenjski cikel razvoja storitev • Referenčni modeli varnostne arhitekture • Tehnologije, povezane s kibernetsko varnostjo • Nadzor kibernetske varnosti in rešitev • Tveganja kibernetske varnosti • Kibernetske grožnje • Trendi kibernetske varnosti • Zahteve glede pravne, regulativne in zakonodajne skladnosti, priporočila in dobre prakse • Postopki kibernetske varnosti • Tehnologije za izboljšanje zasebnosti (PET)

	• Standardi, metodologije in okviri za načrtovanje zasebnosti	
e-kompetence (iz e-CF)	A.5. Arhitekturno oblikovanje A.6. Oblikovanje aplikacij 8.1. Razvoj aplikacij 8.3. Preizkušanje 8.6. Inženiring sistemov IKT	Stopnja 5 Stopnja 3 Stopnja 3 Stopnja 3 Stopnja 4

2.6 RAZISKOVALEC KIBERNETSKE VARNOSTI

Naslov profila	Raziskovalec kibernetske varnosti	
Nadomestni naslov(i)	Revizor za informacijsko varnost (IT ali pravni revizor) Upravljavec skladnosti s tveganji upravljanja (GRC) Revizor področja kibernetske varnosti Pooblaščenec postopkov in procesov kibernetske varnosti Pooblaščenec varnostnega tveganja in skladnosti za varstvo podatkov Analitik za oceno varstva podatkov	
Povzetek izjave	Izvajanje revizije kibernetske varnosti v ekosistemu organizacije. Zagotavljanje skladnosti z zakoni, predpisi, informacijami o politiki, varnostnimi zahtevami, industrijskimi standardi in dobrimi praksami.	
Misija	Izvaja neodvisne preglede za oceno učinkovitosti postopkov in kontrol ter splošne skladnosti s politikami pravnih in regulativnih okvirov organizacije. Ocenjuje, preizkuša in preverja izdelke, povezane s kibernetsko varnostjo (sistemi, strojna oprema, programska oprema in storitve), funkcije in politike, ki zagotavljajo skladnost s smernicami, standardi in predpisi.	
Končni rezultati	• Revizijski načrt za kibernetsko varnost • Revizijsko poročilo o kibernetski varnosti	
Glavna(-a) naloga(-e)	• Razvoj revizijske politike, postopkov, standardov in smernic organizacije • Določitev metodologij in praks, ki se uporabljajo za revizijo sistemov • Vzpostavitev ciljnega okolja in upravljanje revizijskih dejavnosti • Opredelitev obsega revizije, ciljev in meril za revizijo • Priprava revizijskega načrta, v katerem so opisani okviri, standardi, metodologija, postopki in revizijski preskusi; • Pregled cilja ocenjevanja, varnostnih ciljev in zahtev na podlagi profila tveganja • Revizija skladnosti z veljavnimi zakoni in predpisi, povezanimi s kibernetsko varnostjo • Revizijska skladnost z veljavnimi standardi, povezanimi s kibernetsko varnostjo • Izvajanje revizijskega načrta ter zbiranje dokazov in izvedba meritev • Vzdrževanje in varovanje celovitosti revizijskih evidenc • Priprava in posredovanje poročil o ugotavljanih skladnosti, zanesljivosti, reviziji, certificiranju in vzdrževanju • Spremljanje dejavnosti za odpravo tveganj	
Ključne spretnosti	• Organizacija in delo na sistematičen in deterministične način temelječ na dokazih • Spremljanje in praksa revizijskih okvirov, standardov in metodologij • Uporaba revizijskih orodij in tehnik • Analiziranje poslovnih procesov, ocenjevanje in pregledovanje varnosti programske ali strojne opreme ter tehničnih in organizacijskih kontrol • Razčlenitev in analizirati sisteme za odkrivanje pomanjkljivosti in neučinkovitih kontrol • Sporočanje, pojasnjevanje in prilagajanje pravnih in regulativnih zahtev ter poslovnih potreb • Zbiranje, vrednotenje, vzdrževanje in zaščita revizijskih informacij • Integriteta, nepristranska in neodvisna revizija	
Ključno znanje	• Nadzor kibernetske varnosti in rešitve • Zahteve glede pravne, regulativne in zakonodajne skladnosti, priporočila in najboljše prakse • Spremljanje, preskušanje in ocenjevanje učinkovitosti nadzora kibernetske varnosti • Standardi, metodologije in okviri za ugotavljanje skladnosti • Revizijski standardi, metodologije in okviri • Standardi, metodologije in okviri kibernetske varnosti • Certificiranje v zvezi z revizijo • Certifikati iz področja kibernetske varnosti	
e-kompetence (iz e-CF)	B.3. Preizkušanje B.5. Izdelava dokumentacije E.3. Obvladovanje tveganj E.6 Upravljanje kakovosti IKT E.8. Upravljanje informacijske varnosti	Stopnja 4 Stopnja 3 Stopnja 4 Stopnja 4 Stopnja 4

2.7 PREDAVATELJ KIBERNETSKE VARNOSTI

Naslov profila	Predavatelj kibernetske varnosti	
Nadomestni naslov(i)	Strokovnjak za ozaveščanje o kibernetski varnosti Trener za kibernetsko varnost Fakulteta za kibernetsko varnost (profesor, predavatelj)	
Povzetek izjave	Izboljšuje znanje, spretnosti in kompetence ljudi na področju kibernetske varnosti.	
Misija	Oblikuje, razvija in izvaja programe ozaveščanja, usposabljanja in izobraževanja na področju kibernetske varnosti in tem, povezanih z varstvom podatkov. Uporablja ustrezne metode, tehnike in instrumente poučevanja in usposabljanja za komuniciranje in krepitev kulture, zmogljivosti, znanja in spretnosti človeških virov na področju kibernetske varnosti. Spodbuja pomen kibernetske varnosti in jo utrjuje v organizaciji.	
Končni rezultati	• Program ozaveščanja o kibernetski varnosti • Gradivo za usposabljanje na področju kibernetske varnosti	
Glavna(-a) naloga(-e)	• Razvoj, posodabljanje in zagotavljanje učnih načrtov za kibernetsko varnost in varstvo podatkov ter izobraževalnega gradiva za usposabljanje in ozaveščanje na podlagi vsebine, metode, orodij in potreb udeležencev usposabljanja • Organizacija, oblikovanje in izvajanje dejavnosti ozaveščanja na področju kibernetske varnosti in varstva podatkov, seminarjev, tečajev, praktičnega usposabljanja • Spremljanje, ocenjevanje in poročanje o učinkovitosti usposabljanja • Ocena uspešnosti pripravnika in poročanje o njem • Iskanje novih pristopov k izobraževanju, usposabljanju in ozaveščanju • Oblikovanje, razvoj in zagotavljanje simulacij kibernetske varnosti, virtualnih laboratorijev ali okolja kibernetskega dosega • Zagotavljanje smernic za certifikacijske programe za kibernetsko varnost za posameznike • Stalno vzdrževanje in izboljševanje strokovnega znanja; spodbujanje in krepitev stalnega izboljševanja zmogljivosti in zmogljivosti na področju kibernetske varnosti	
Ključne spretnosti	• Opredelitev potreb na področju ozaveščenosti o kibernetski varnosti, usposabljanja in izobraževanja • Oblikovanje, razvoj in izvajanje učnih programov za kritje potreb po kibernetski varnosti • Razviti vaje za kibernetsko varnost, vključno s simulacijami, ki uporabljajo okolja kibernetskega dosega • Zagotavljanje usposabljanja na področju kibernetske varnosti in strokovnega certificiranja na področju varstva podatkov • Uporaba obstoječih virov usposabljanja v zvezi s kibernetsko varnostjo • Razvoj ocenjevalnih programov za dejavnosti ozaveščanja, usposabljanja in izobraževanja • Obveščanje in predstavitev ustreznih deležnikov ter poročanje o njih	
Ključno znanje	• Pedagoški standardi, metodologije in okviri • Ozaveščanje o kibernetski varnosti, razvoj programov izobraževanja in usposabljanja • Certifikati v zvezi s kibernetsko varnostjo • Standardi, metodologije in okviri za izobraževanje in usposabljanje na področju kibernetske varnosti • Zakoni, predpisi in zakonodaja, povezani s kibernetsko varnostjo • Priporočila in najboljše prakse na področju kibernetske varnosti • Standardi, metodologije in okviri za kibernetsko varnost • Nadzor kibernetske varnosti in rešitve	
e-kompetence (iz e-CF)	D.3. Zagotavljanje izobraževanja in usposabljanja D.9. Razvoj osebja E.8. Upravljanje informacijske varnosti	Stopnja 3 Stopnja 3 Stopnja 3

2.8 IZVAJALEC KIBERNETSKE VARNOSTI

Naslov profila	Izvajalec kibernetske varnosti	
Nadomestni naslov(i)	Izvajalec informacijske varnosti Strokovnjak za rešitve kibernetske varnosti Razvijalec kibernetske varnosti Inženir za kibernetsko varnost Inženir za razvoj, varnost in delovanje (DevSecOps)	
Povzetek izjave	Razvoj, uvajanje in upravljanje rešitev za kibernetsko varnost (sistemov, sredstev, programske opreme, kontrol in storitev) v zvezi z infrastrukturami in proizvodi.	
Misija	Zagotavlja tehnični razvoj, integracijo, preskušanje, izvajanje, delovanje, vzdrževanje, spremljanje in podporo kibernetskih rešitev, povezanih s kibernetsko varnostjo. Zagotavlja skladnost s specifikacijami in zahtevami glede skladnosti, zagotavlja dobro delovanje in rešuje tehnična vprašanja, ki jih organizacija zahteva v rešitvah, povezanih s kibernetsko varnostjo (sistemi, sredstva, programska oprema, kontrole in storitve), infrastruktura in izdelki.	
Končni rezultati	• Rešitve za kibernetsko varnost	
Glavna(-a) naloga(-e)	• Razvoj, izvajanje, vzdrževanje, nadgradnja, testiranje izdelkov kibernetske varnosti • Zagotavljanje podpore uporabnikom in strankam v zvezi s kibernetsko varnostjo • Integrirati rešitve za kibernetsko varnost in zagotoviti njihovo dobro delovanje • Varno konfigurirajte sisteme, storitve in izdelke • Vzdrževanje in nadgradnja varnosti sistemov, storitev in izdelkov • Izvajati postopke in kontrole na področju kibernetske varnosti • Spremljanje in zagotavljanje uspešnosti izvedenih kontrol kibernetske varnosti • Dokumentiranje in poročila o varnosti sistemov, storitev in izdelkov • Tesno sodelovanje z osebjem IT/OT pri ukrepih kibernetske varnosti • Izvajanje in upravljanje varnostnih popravkov izdelkov za odpravljanje tehničnih šibkih točk	
Ključne spretnosti	• Obveščanje ustreznih deležnikov • Vključevanje rešitev kibernetske varnosti v infrastrukturo organizacije • Konfiguriranje rešitve v skladu z varnostno politiko organizacije • Ocena varnosti in učinkovitosti rešitev • Razvoj kode, skript in programov • Reševanje vprašanj kibernetske varnosti • Sodelovanje z drugimi člani skupine in sodelavci	
Ključno znanje	• Varen življenjski cikel razvoja • Računalniško programiranje • Varnost operacijskih sistemov • Varnost računalniških omrežij • Nadzor kibernetske varnosti in rešitve • Ofenzivne in obrambne varnostne prakse • Priporočila za varno kodiranje in dobre prakse • Priporočila in dobre prakse na področju kibernetske varnosti • Standardi, metodologije in okviri preizkušanja • Preizkusni postopki • Tehnologije, povezane s kibernetsko varnostjo	
e-kompetence (iz e-CF)	A.5. Arhitekturno oblikovanje A.6. Oblikovanje aplikacij 8.1. Razvoj aplikacij 8.3. Preizkušanje 8.6. Inženiring sistemov IKT	Stopnja 3 Stopnja 3 Stopnja 3 Stopnja 3 Stopnja 4

2.9 RAZISKOVALEC KIBERNETSKE VARNOSTI

Naslov profila	Raziskovalec kibernetske varnosti	
Nadomestni naslov(i)	Inženir za raziskave kibernetske varnosti Direktor za raziskave na področju kibernetske varnosti Višji uradnik za raziskave na področju kibernetske varnosti Uradnik za raziskave in razvoj na področju kibernetske varnosti Znanstveno osebje na področju kibernetske varnosti Uradnik za raziskave in inovacije/strokovnjak za kibernetsko varnost Raziskovalna sodelavka na področju kibernetske varnosti	
Povzetek izjave	Raziskovanje področja kibernetske varnosti in vključevanje rezultatov v rešitve na področju kibernetske varnosti.	
Misija	Izvajanje temeljnih raziskav ter spodbuja inovacije na področju kibernetske varnosti s sodelovanjem z drugimi deležniki. Analiziranje trendov in znanstvenih dognanj na področju kibernetske varnosti.	
Končni rezultati	• Objava na področju kibernetske varnosti	
Glavna(-a) naloga(-e)	• Analiziranje in ocenjevanje tehnologij, rešitev, razvoja ter procesov na področju kibernetske varnosti • Izvajanje raziskovalno - razvojnega dela v zvezi s temami, povezanimi s kibernetsko varnostjo - nove ideje za raziskave in inovacije • Pospeševanja napredka pri aktualnih temah kibernetske varnosti • Pomoč pri razvoju inovativnih rešitev kibernetske varnosti • Izvajati preizkuse, razvijati konceptne in pilotne rešitve ter prototipe kibernetske varnosti • Izbira in uporaba okvirov, metod, standardov, orodij in protokolov • Prispevati k najsodobnejšim poslovnim idejam, storitvam in rešitvam na področju kibernetske varnosti • Pomoč pri krepitvi zmogljivosti na področju kibernetske varnosti, vključno z ozaveščanjem, teoretičnim in praktičnim usposabljanjem, testiranjem, mentorstvom, nadzorom in izmenjavo znanj ter izkušenj; • Opredeliti medsektorske dosežke na področju kibernetske varnosti in jih uporabiti v inovativnih pristopih in rešitvah; • Vodenje ali sodelovanje v inovacijskih procesih in projektih, vključno z vodenjem projektov in pripravo proračuna • Objavljanje in predstavljanje znanstvenih del ter rezultatov raziskav in razvoja	
Ključne spretnosti	• Ustvarjanje novih idej in prenos teorije v prakso • Razčleniti in analizirati sisteme za odkrivanje pomanjkljivosti in neučinkovitih kontrol • Razčleniti in analizirati sisteme za podajanje zahtev področja varnosti in zasebnosti ter definirati učinkovite rešitve • Spremljanje napredka na področju tehnologij kibernetske varnosti • Obveščanje ustreznih deležnikov • Reševanje vprašanj, povezanih s kibernetsko varnostjo • Sodelujte z drugimi člani skupine in sodelavci	
Ključno znanje	• Raziskave, razvoj in inovacije, povezane s kibernetsko varnostjo • Standardi, metodologije in okviri za kibernetsko varnost • Pravne, regulativne in zakonodajne zahteve za sprostitev ali uporabo tehnologij, povezanih s kibernetsko varnostjo • Multidisciplinarni vidik kibernetske varnosti • Postopki za razkritje odgovornih informacij	
e-kompetence (iz e-CF)	A.7. Spremljanje tehnoloških trendov A.9. Inoviranje D.7. Podatkovna znanost in analitika C.4. Obvladovanje težav D.10. Upravljanje informacij in znanja	Stopnja 5 Stopnja 5 Stopnja 4 Stopnja 3 Stopnja 3

2.10 VODJA TVEGANJ KIBERNETSKE VARNOSTI

Naslov profila	Vodja tveganj kibernetske varnosti	
Nadomestni naslov(i)	Analitik tveganja na področju informacijske varnosti Svetovalec za ugotavljanje tveganj kibernetske varnosti Analitik tveganja za kibernetsko varnost Upravitelj kibernetskega tveganja	
Povzetek izjave	Obvladovanje tveganj, povezanih s kibernetsko varnostjo organizacije, v skladu s strategijo organizacije. Razvijati, vzdrževati in sporočati postopke za obvladovanje tveganj kibernetske varnosti.	
Misija	Upravljanje (identifikacija, analizira, ocenjevanje, zmanjšuje) tveganja kibernetske varnosti infrastrukture, sistemov in storitev IKT. Z načrtovanjem, uporabo, poročanjem, analizo, ocenjevanjem in obravnavanjem tveganj. Določati strategijo obvladovanja tveganja za organizacijo in zagotavlja, da tveganja ostanejo na sprejemljivi ravni za organizacijo, z izbiro ukrepov zmanjševanja tveganja in nadzora.	
Končni rezultati	• Poročilo o oceni tveganja za kibernetsko varnost • Akcijski načrt za odpravo tveganj na področju kibernetske varnosti	
Glavna(-a) naloga(-e)	• Razvoj strategije organizacije za obvladovanje tveganj na področju kibernetske varnosti • Upravljanje popisa sredstev organizacije • Opredelitev in ocena groženj in ranljivosti sistemov IKT, z vidika kibernetske varnosti • Opredelitev groženj okolja, vključno s profili napadalcev in oceno potenciala napadov • Oceniti tveganja kibernetske varnosti in podajanje predlogov za obravnavo tveganj, vključno z varnostnim nadzorom, zmanjševanjem in izogibanjem tveganju, kot so obravnavani v strategiji organizacije • Spremljanje učinkovitosti nadzora kibernetske varnosti in ravni tveganja • Zagotoviti, da tveganja kibernetske varnosti ostanejo na sprejemljivi ravni za organizacijo; • Razvoj, vzdrževanje, poročanje tekom celotnega cikla obvladovanja tveganj	
Ključne spretnosti	• Izvajati okvire, metodologije in smernice za obvladovanje tveganj za kibernetsko varnost ter zagotoviti skladnost s predpisi in standardi • Analiza in krepitev praks organizacije obvladovan tveganj kibernetske varnosti • Lastnikom poslovnih sredstev, vodstvenim delavcem in drugim deležnikom omogočiti sprejemanje odločitev, ki temeljijo informacijah za obvladovanje in zmanjševanje tveganj. • Vzpostavitev okolja, zavedajočega se tveganj področja kibernetske varnosti • Obveščanje ustreznih deležnikov • Predlagati in upravljati možnosti delitve tveganja	
Ključno znanje	• Standardi, metodologije in okviri za obvladovanje tveganj • Orodja za obvladovanje tveganj • Priporočila za obvladovanje tveganja in dobre prakse • Kibernetske grožnje • Ranljivosti računalniških sistemov • Rešitve nadzora kibernetske varnosti • Tveganja za kibernetsko varnost • Spremljanje, preskušanje in ocenjevanje učinkovitosti nadzora kibernetske varnosti • Certifikati iz področja kibernetske varnosti • Tehnologije, povezane s kibernetsko varnostjo	
e-kompetence (iz e-CF)	E.3. Obvladovanje tveganj E.5. Izboljšanje postopka E.7. Upravljanje poslovnih sprememb E.9. IS-upravljanje	Stopnja 4 Stopnja 3 Stopnja 4 Stopnja 4

2.11 PREISKOVALEC DIGITALNE FORENZIKE

Naslov profila	**Preiskovalec digitalne forenzike**	
Nadomestni naslov(i)	Digitalni forenzični analitik za kibernetsko varnost Specialist za računalniško forenziko Svetovalec za računalniško forenziko	
Povzetek izjave	Zagotoviti, da bo preiskava kibernetske kriminalitete razkrila vse digitalne dokaze za dokazovanje zlonamerne dejavnosti.	
Misija	Povezuje artefakte s fizičnimi osebami, zajema, pridobiva, identificira in hrani podatke, vključno z manifestacijami, vložki, izhodi in procesi digitalnih sistemov, ki se preiskujejo. Zagotavlja analizo, rekonstrukcijo in razlago digitalnih dokazov na podlagi kvalitativnega mnenja. Predstavlja nepristranski kvalitativni pogled brez razlage pridobljenih ugotovitev.	
Končni rezultati	• Rezultati analize digitalne forenzike • Elektronski dokazi	
Glavna(-a) naloga(-e)	• Razvoj politike, načrtov in postopkov raziskovanja digitalne forenzike • Opredelitev, obnovitev, pridobivanje, dokumentiranje in analiza digitalnih dokazov • Ohraniti in zaščititi digitalne dokaze ter jih dati na voljo pooblaščenim deležnikom • Pregled okolij za dokaze o nedovoljenih in nezakonitih dejanjih • Sistematično in deterministično dokumentiranje, poročanje in predstavitev ugotovitev in rezultatov digitalne forenzične analize • Izbira in prilagajanje forenzičnega testiranja, analiziranja in poročanja	
Ključne spretnosti	• Etično in neodvisno delo od notranjih ali zunanjih akterjev • Zbiranje informacij ob ohranjanju celovitosti sistemov • Opredelitev, analiza in korelacija dogodkov na področju kibernetske varnosti • Pojasnitev in predstavitev digitalnih dokaz na preprost, enostaven in lahko razumljiv način • Priprava podrobnih in temeljitih poročil o preiskavah	
Ključno znanje	• Priporočila za digitalno forenziko in dobre prakse • Standardi, metodologije in okviri za digitalno forenziko • Postopki analize digitalne forenzike • Preskusni postopki • Postopki kazenskih preiskav, standardi, metodologije in okviri • Zakoni, predpisi in zakonodaja, povezani s kibernetsko varnostjo • Orodja za analizo zlonamerne programske opreme • Kibernetske grožnje • Ranljivosti računalniških sistemov • Postopki napadov na kibernetsko varnost • Varnost operacijskih sistemov • Varnost računalniških omrežij • Certifikati s področja kibernetske varnosti	
e-kompetence (iz e-CF)	A.7. Spremljanje tehnoloških trendov B.3. Preizkušanje B.5. Izdelava dokumentacije E.3. Obvladovanje tveganj	Stopnja 3 Stopnja 4 Stopnja 3 Stopnja 3

2.12 IZVAJALEC PENETRACIJSKIH TESTOV

Naslov profila	Izvajalec penetracijskih testov	
Nadomestni naslov(i)	Pentester Etični Hacker Analitik ranljivosti Preizkuševalec kibernetske varnosti Strokovnjak za kibernetske napade Strokovnjak za obrambno pred kibernetskimi napadi Strokovnjak Rdeče skupine Red Teamer	
Povzetek izjave	Ocenjevanje učinkovitosti varnostnih kontrol, odkrivanje ranljivosti kibernetske varnosti ter ocenjevanje njihove kritičnost, v primeru kibernetskega napada s strani sovražnih akterjev.	
Misija	Načrtuje, oblikuje in izvaja aktivnosti penetracijskega testiranja ter scenarijev napadov za oceno učinkovitosti uvedenih ali načrtovanih varnostnih ukrepov. Opredelitev ranljivosti ali napak pri tehničnih in organizacijskih kontrolah, ki vplivajo na zaupnost, celovitost in razpoložljivost proizvodov IKT (npr. sistemov, strojne opreme, programske opreme in storitev).	
Končni rezultati	• Poročilo o rezultatih ocene ranljivosti • Poročilo o testiranju penetracije	
Glavna(-a) naloga(-e)	• Opredelitev, analiza in ocena tehničnih in organizacijskih ranljivosti na področju kibernetske varnosti • Prepoznavanje vektorjev napadov, odkrivanje in dokazovanje izkoriščanja tehničnih ranljivosti na področju kibernetske varnosti • Preskušanje sistemov v skladu z regulativnimi standardi • Izbira in razvoj ustreznih tehnik penetracijskega testiranja • Organiziranje testnih načrtov in postopkov za penetracijsko testiranje • Vzpostavljanje postopkov za analizo rezultatov penetracijskega testiranja in poročanja • Dokumentiranje in poročanje deležnikom o rezultatih penetracijskega testiranja • Uvajanje orodij za testiranje penetracijskih testov in testnih programov	
Ključne spretnosti	• Razviti kode, skripte in programe • Izvajati socialni inženiring • Prepoznavanje in izkoriščanje ranljivosti • Izvajanje etičnega hekanja • Razmišljajte ustvarjalno in zunaj škatle • Opredelitev in reševanje vprašanj, povezanih s kibernetsko varnostjo • Obveščanje in predstavitev ustreznih deležnikov ter poročanje o njih • Učinkovito uporabljati orodja za testiranje penetracije • Izvajati tehnično analizo in poročanje • Razgraditi in analizirati sisteme za odkrivanje pomanjkljivosti in neučinkovitih kontrol • Pregledovanje kode in njihove varnosti	
Ključno znanje	• Postopki napadov na kibernetsko varnost • Naprave informacijske tehnologije (IT) in operativne tehnologije (OT) • Ofenzivni in obrambni varnostni postopki • Varnost operacijskih sistemov • Varnost računalniških omrežij • Postopki penetracijskega testiranja • Standardi, metodologije in okviri penetracijskega testiranja • Orodja za penetracijsko testiranje • Računalniško programiranje • Ranljivosti računalniških sistemov • Priporočila in najboljše prakse na področju kibernetske varnosti • Certifikati iz področja kibernetske varnosti	
e-kompetence (iz e-CF)	8.2. Vključevanje sestavnih delov 8.3. Preizkušanje 8.4. Uvedba rešitve 8.5. Izdelava dokumentacije 8.6. E.3. Obvladovanje tveganj	Stopnja 4 Stopnja 4 Stopnja 2 Stopnja 3 Stopnja 4

3. KNJIŽNICA KONČNIH IZDELKOV

Seznam končnih rezultatov vsebuje nekaj okvirnih in praktičnih primerov rezultatov/izvlečkov za vsak profil vloge. Navedeni rezultati so izbrani primeri, saj seznam ni popoln in ne zajema vseh vidikov vseh naštetih profilov.

Naslov profila	Končni rezultat	Opis
Vodja informacijske varnosti (CISO)	Strategija za kibernetsko varnost	Strategija kibernetske varnosti je načrt ukrepov za izboljšanje varnosti, odpornosti infrastrukture in storitev organizacije na kibernetske napade.
Vodja informacijske varnosti (CISO)	Politika kibernetske varnosti	Pravila za uvrstitev na seznam politik za zagotovitev kibernetske varnosti organizacije.
Upravitelj v primeru kibernetskih napadov	Načrt odzivanja na incidente	Sklop dokumentiranih postopkov, v katerih so podrobno opisani koraki, ki jih je treba sprejeti v vsaki fazi odziva na incident (priprava, odkrivanje in analiza, zadrževanje, izkoreninjenje in okrevanje, dejavnost po incidentu).
Upravitelj v primeru kibernetskih napadov	Poročilo o kibernetskih incidentih	Poročilo s podrobnostmi o enem ali več kibernetskih incidentih.
Pooblaščenec za pravne zadeve, politiko in skladnost v kibernetskem prostoru	Priročnik o skladnosti	Priročnik, ki zagotavlja temeljito razumevanje obveznosti organizacije glede skladnosti z zakonodajo. Vključuje lahko notranje politike ali postopke za zagotavljanje skladnosti z zakoni, predpisi in/ali standardi.
Pooblaščenec za pravne zadeve, politiko in skladnost v kibernetskem prostoru	Poročilo o skladnosti	Poročilo, v katerem je predstavljeno trenutno stanje položaja organizacije glede skladnosti.
Strokovnjak za kibernetske grožnje	Obveščevalni priročnik o kibernetskih grožnjah (ali priročnik)	Priročnik z orodji in/ali metodologijami za zbiranje in/ali izmenjavo obveščevalnih podatkov o kibernetskih grožnjah.
Strokovnjak za kibernetske grožnje	Poročilo o kibernetski grožnji	Poročilo o glavnih grožnjah, glavnih trendih, opaženih v zvezi z grožnjami, akterjih groženj in/ali tehnikah napadov. Poročilo lahko vključuje tudi ustrezne blažilne ukrepe.
Arhitekt kibernetske varnosti	Diagram arhitekture kibernetske varnosti	Vizualna predstavitev arhitekture sistema kibernetske varnosti organizacije, ki se uporablja za zaščito sredstev pred kibernetskimi napadi.
Arhitekt kibernetske varnosti	Kibernetska varnost Poročilo o zahtevah	Poročilo, v katerem je naveden sklop zahtev, potrebnih za zagotavljanje kibernetske varnosti sistema.
Revizor za kibernetsko varnost	Revizijski načrt za kibernetsko varnost	Načrt, v katerem so predstavljeni splošna strategija in postopki, ki jih bo revizor uporabil za izvedbo revizije kibernetske varnosti.
Revizor za kibernetsko varnost	Revizijsko poročilo o kibernetski varnosti	Poročilo z natančnim razumevanjem ravni varnosti sistema, v katerem so ocenjene njegove prednosti in slabosti na področju kibernetske varnosti. Prav tako lahko zagotovi sanacijske ukrepe za izboljšanje splošne kibernetske varnosti sistema.
Predavatelj kibernetske varnosti	Program ozaveščanja o kibernetski varnosti	Program dejavnosti za ozaveščanje o vprašanjih, povezanih s kibernetsko varnostjo (npr. predavanja o napadih)

		in grožnje) pomagati organizacijam pri preprečevanju in zmanjševanju s tem povezanih tveganj za kibernetsko varnost.
Predavatelj kibernetske varnosti	Gradivo za usposabljanje na področju kibernetske varnosti	Gradivo, ki pojasnjuje koncepte, metodologije in orodja, povezane s kibernetsko varnostjo, za usposabljanje ali izpopolnjevanje posameznikov. Vključuje lahko priročnike za učitelje, nabore orodij za učence in/ali virtualne slike za podporo pri usposabljanju.
Izvajalec kibernetske varnosti	Rešitve za kibernetsko varnost	Rešitve za kibernetsko varnost lahko vključujejo orodja in storitve, katerih cilj je zaščititi organizacije pred kibernetskimi napadi.
Raziskovalec kibernetske varnosti	Publikacija na področju kibernetske varnosti	Akademska publikacija, ki objavlja ugotovitve in rezultate raziskav v okviru kibernetske varnosti. Namen publikacije bi lahko bil napredek tehnologije in/ali razvoj novih inovativnih rešitev.
Vodja tveganj kibernetske varnosti	Poročilo o oceni tveganja za kibernetsko varnost	Poročilo, v katerem so navedeni rezultati ugotavljanja, analize in ocene tveganj za kibernetsko varnost sistema. Vključuje lahko tudi kontrole za zmanjšanje ali zmanjšanje ugotovljenih tveganj na sprejemljivo raven.
Vodja tveganj kibernetske varnosti	Tveganje za kibernetsko varnost Akcijski načrt za sanacijo	Akcijski načrt, v katerem so navedene dejavnosti, povezane z izvajanjem blažilnih ukrepov za zmanjšanje tveganj za kibernetsko varnost.
Vodja tveganj kibernetske varnosti	Rezultati analize digitalne forenzike	Rezultati analize digitalnih podatkov, ki razkrivajo morebitne dokaze o zlonamernih incidentih in prepoznavajo možne akterje na področju groženj.
Preiskovalec digitalne forenzike	Elektronski dokazi	Morebitni dokazi, ki izhajajo iz podatkov, ki jih vsebuje ali proizvede katera koli naprava, katerih delovanje je odvisno od programske opreme ali podatkov, shranjenih ali prenesenih prek računalniškega sistema ali omrežja. (npr. natančno zbiranje hlodov)
Izvajalec penetracijskih testov	Poročilo o testiranju penetracijskega testa	Poročilo navaja in ocenjuje kritičnost šibkih točk, odkritih v sistemu med (običajno samodejnim) skeniranjem ranljivosti. Poročilo lahko predlaga tudi osnovne sanacijske ukrepe.
Izvajalec penetracijskih testov	Poročilo o testiranju penetracijskega testa	Poročilo, ki vsebuje podrobno in celovito analizo ranljivosti sistema, ugotovljenih med varnostnim testiranjem. Poročilo lahko vključuje tudi predlagane sanacijske ukrepe.

TP-09–22–510-EN-

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost ENISA je agencija Unije, ki si prizadeva doseči visoko skupno raven kibernetske varnosti po vsej Evropi. Agencija Evropske unije za kibernetsko varnost, ki je bila ustanovljena leta 2004 in okrepljena z aktom EU o kibernetski varnosti, prispeva k kibernetski politiki EU, povečuje zanesljivost proizvodov, storitev in postopkov IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi pri pripravi na kibernetske izzive prihodnosti. Agencija z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter nazadnje ohranila digitalno varnost evropske družbe in državljanov. Več informacij o agenciji ENISA in njenem delu je na voljo na: www.enisa.europa.eu.

ENISA
Agencija Evropske unije za kibernetsko varnost

Pisarna v Atenah
Agamemnos 14, Chalandri 15231, Attiki, Grčija

Pisarna Heraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grčija

enisa.europa.eu □ nma

ISBN: 978–92–9204–584–5
DOI: 10.2824/859537