Špeciálna publikácia NIST č. 800-181
Verzia 1

Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

Táto publikácia je voľne dostupná na:
https://doi.org/10.6028/NIST.SP.800-181r1

National Institute of Standards and Technology
U.S. Department of Commerce

Špeciálna publikácia č. 800-181
Verzia 1

Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia)

Rodney Petersen (riaditeľ)
Danielle Santos (manažérka pre komunikáciu a riadenie)
Karen A. Wetzel (manažérka pre NICE koncepciu)
Národná iniciatíva pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE)
Oddelenie aplikovanej kybernetickej bezpečnosti
Laboratórium informačných technológií

Matthew C. Smith
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

Táto publikácia je voľne dostupná na:
https://doi.org/10.6028/NIST.SP.800-181r1

November 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Autorstvo dokumentu

Táto publikácia bola vytvorená Národným inštitútom pre štandardy a technológie (*angl. skr. NIST*) v súlade so svojimi zákonnými povinnosťami podľa Federálneho zákona o modernizácii informačnej bezpečnosti (*angl. skr. FISMA*) z roku 2014, 44 U.S.C. § 3551 *a nasl.*, Verejné právo (*angl. skr. P.L.*) 113-283. NIST je zodpovedný za vypracovanie noriem a usmernení pre informačnú bezpečnosť vrátane minimálnych požiadaviek na federálne informačné systémy. Takéto normy a usmernenia sa nevzťahujú na vnútroštátne bezpečnostné systémy bez schválenia príslušných úradov vykonávajúcich politickú moc nad takýmito systémami. Toto usmernenie je v súlade s požiadavkami obežníka Úradu pre riadenie a rozpočet (*angl. Office of Management and Budget, OMB*) A-130.

Obsah z tejto publikácie nesmie byť použitý na účely, ktoré by boli v rozpore s normami a usmerneniami ustanovenými ministrom obchodu na základe zákonnej právomoci. Tieto usmernenia nesmú byť chápané tak, že menia alebo nahrádzajú existujúce právomoci ministra obchodu, riaditeľa OMB alebo akéhokoľvek iného úradu. Táto publikácia môže byť použitá mimovládnymi organizáciami na dobrovoľnom základe a nepodlieha autorskému právu v Spojených štátoch amerických. Autorstvo dokumentu náleží NIST.

National Institute of Standards and Technology Special Publication 800-181
Natl. Inst. Stand. Technol. Spec. Publ. 800-181 Rev. 1, 27 strán (November 2020)
CODEN: NSPUE2

Táto publikácia je voľne dostupná na adrese:
https://doi.org/10.6028/NIST.SP.800-181r1

V tomto dokumente môžu byť identifikované obchodné subjekty, zariadenia alebo materiály s cieľom primerane opísať experimentálny postup alebo koncepciu. Takáto identifikácia nie je určená na to, aby implikovala odporúčanie alebo schválenie inštitútom NIST, a taktiež nie je určená na to, aby naznačovala, že spomenuté subjekty, materiály alebo zariadenia sú nevyhnutne najlepšie na použitie pre tento účel.

V tejto publikácii môžu byť odkazy na iné publikácie, ktoré v súčasnosti NIST vyvíja v súlade s pridelenými zákonnými povinnosťami. Informácie v tejto publikácii vrátane pojmov a metodík môžu federálne agentúry používať ešte pred dokončením takýchto sprievodných publikácií. Do momentu dokončenia každej publikácie zostávajú v platnosti aktuálne požiadavky, usmernenia a postupy, ak existujú. Na účely plánovania a zapracovania zmien môžu federálne agentúry sledovať vývoj týchto nových publikácií v rámci NIST.

Pripomienky a komentáre všetkých pracovných verzií publikácií počas obdobia verejného pripomienkovania je zo strany NIST vítaná. Ďalšie publikácie NIST o kybernetickej bezpečnosti sú k dispozícii na https://csrc.nist.gov/publications.

Komentáre a pripomienky k tejto publikácii je možné zasielať na adresu:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: NICEFramework@nist.gov

Všetky komentáre a pripomienky podliehajú zverejneniu podľa zákona o verejnom prístupe k informáciám (FOIA).

Správy o informačných technológiách

Laboratórium informačných technológií (*angl. Information Technology Laboratory, ITL*) v NIST podporuje americkú ekonomiku a verejné blaho tým, že poskytuje technické zázemie pre Národnú infraštruktúru štandardov a meraní. ITL vyvíja testy, testovacie metódy, referenčné údaje, štúdie uskutočniteľnosti o implementácii koncepcie vrátane technických analýz na podporu vývoja a produktívneho využívania informačných technológií. Medzi zodpovednosti ITL patrí vypracovanie riadiacich, administratívnych, technických a fyzických noriem a usmernení pre efektívnu bezpečnosť a zabezpečenie súkromia iných ako federálnych informačných systémov pre spracovanie údajov. Špeciálna publikácia série 800 popisuje informácie o výskume, usmerneniach a osvetovom úsilí ITL v oblasti bezpečnosti informačných systémov a spolupráce s priemyslom, vládou a akademickými organizáciami.

Abstrakt

Táto publikácia Národnej iniciatívy pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE) definuje Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia) ako základný dokument pre popis a zdieľanie informácií súvisiacich s kybernetickou bezpečnosťou. Popisuje prácu vo forme pracovných úloh a príslušné znalosti a zručnosti, ktoré slúžia ako základ pre vzdelávanie v oblasti kybernetickej bezpečnosti určené študentom, záujemcom o prácu a zamestnancom. Definované kompetencie sú určené pre stanovenie znalostí a zručností študentov v procese vzdelávania, záujemcom o prácu a zamestnancom na preukázanie požadovaných profesijných schopností. Rovnako ako v prípade katalógov zručností pomôže NICE koncepcia v procese identifikácie, získania, rozvoja a udržania si zamestnancov v oblasti kybernetickej bezpečnosti. Kompetenčný rámec pre kybernetickú bezpečnosť tvorí referenčný dokument na základe ktorého môžu organizácie a sektorové autority definovať ďalšie materiály a nástroje pre podporu rôznych aspektov vzdelávania v oblasti kybernetickej bezpečnosti a ďalšieho vzdelávania.

Kľúčové slová

Kompetencia, kybernetická bezpečnosť, kybernetický priestor, vzdelávanie, znalosť, rola, bezpečnosť, zručnosť, úloha, tím, tréning, zamestnanci (kapacity), pracovná rola.

Autorské práva

POZNÁMKA: Laboratórium informačných technológií (ITL) požiadalo, aby držitelia patentových nárokov, ktorých použitie sa môže vyžadovať na dosiahnutie súladu s pokynmi alebo požiadavkami tejto publikácie, oznámili tieto patentové nároky ITL. Vlastníci patentov však nie sú povinní reagovať na výzvy ITL a ITL nevykonalo patentovú rešerš za účelom zistenia, ktoré patenty sa môžu vzťahovať na túto publikáciu.

Ku dňu zverejnenia publikácie neboli na základe výzvy na identifikáciu patentových nárokov, ktorých použitie môže byť potrebné na dosiahnutie súladu s pokynmi alebo požiadavkami tejto publikácie, ITL identifikované žiadne takéto patentové nároky.

ITL nezaručuje, že príslušné licencie nie sú potrebné z dôvodu ochrany autorských práv pri používaní tejto publikácie

Konvencie použité v dokumente

V NICE koncepcii sa na osoby, ktoré vykonávajú prácu v oblasti kybernetickej bezpečnosti – vrátane študentov, uchádzačov o zamestnanie a zamestnancov – odkazuje pojmom aktér. Tento pojem zdôrazňuje, že každá osoba vykonávajúca odbornú prácu v oblasti kybernetickej bezpečnosti je zároveň celoživotným študentom.

Poďakovanie

NICE koncepcia bola vyvinutá hlavným autorským tímom, ktorý zahŕňa zástupcov z mnohých oddelení a agentúr vo federálnej vláde Spojených štátov amerických. Národný inštitút pre štandardy a technológie (NIST) chce poďakovať nasledujúcim členom tímu, ktorých úsilie významne prispelo k tejto publikácii:

William Newhouse, Národný inštitút pre štandardy a technológie
Pam Frugoli, Ministerstvo práce
Lisa Dorr, Ministerstvo vnútornej bezpečnosti
Kenneth Vrooman, Agentúra pre kybernetickú bezpečnosť a bezpečnosť infraštruktúry
Bobbie Sanders, Ministerstvo obrany
Patrick Johnson, Ministerstvo obrany
Matt Isnor, Ministerstvo obrany
Stephanie Shively, Ministerstvo obrany
Ryan Farr, Ministerstvo obrany

Autori a autorský tím ďakujú za významné príspevky jednotlivcov a organizácií vo verejnom a súkromnom sektore, ktorých zmysluplné a konštruktívne komentáre zlepšili celkovú kvalitu, presnosť a užitočnosť tejto publikácie. Autori oceňujú najmä množstvo užitočných odpovedí na žiadosť o pripomienky ku koncepcii NICE a tiež aj verejné pripomienky k predbežnej verzii tejto publikácie.

Okrem toho, tím oceňuje príspevky tých, ktorí vytvorili predchádzajúce vydania národných kompetenčných rámcov v oblasti kybernetickej bezpečnosti tak, ako je to uvedené na stránke zdrojov ku koncepcii NICE, v časti história. [1]

Poznámka pre čitateľov

Vitajte v dokumente Kompetenčný rámec pre kybernetickú bezpečnosť Národnej iniciatívy pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE) verzie 1. Pracovníci programu NICE dostali od komunity rozsiahlu spätnú väzbu vrátane odpovedí na nedávne porovnanie všeobecných prostriedkov týkajúcich sa rámca NICE a tiež odpovedí na verejný návrh tohto verejného dokumentu. Vzhľadom na uvedenú spätnú väzbu a prepojený ekosystém kybernetickej bezpečnosti sa autorský tím rozhodol prijať a podporovať atribúty agility, flexibility, interoperability a modularity. Tieto atribúty viedli k prepracovaniu NICE koncepcie s cieľom poskytnúť zjednodušený prístup k rozvoju pracovnej sily na riadenie rizika kybernetickej bezpečnosti. Nižšie je uvedený sumár zmien:

- Organizácia konštruktov vo Verzii 1 bola zjednodušená vynechaním kategórií (napr. bezpečné poskytovanie, dohľad a riadenie, ochrana a obrana, analýza atď.) a špeciálnych oblastí použitia (napr. reakcia na incidenty, analýza hrozieb, riadenie kybernetickej bezpečnosti atď.). S cieľom zjednodušiť prístup, ktorý poskytuje organizáciám agilitu, flexibilitu, interoperabilitu a modularitu, definuje Verzia 1 zjednodušený súbor stavebných blokov pozostávajúci z úloh, znalostí a zručností. Organizácie, ktorým vyhovuje predchádzajúce členenie podľa kategórií a špeciálnych oblastí použitia ich môžu naďalej používať alebo vytvárať pracovné skupiny na základe týchto konceptov a zosúladiť ich s touto verziou NICE koncepcie (pozri kapitolu 3.4).
- Verzia 1 opisuje niekoľko použití úloh, znalostí a zručností vrátane metód aplikácie, ktoré sú definované v pracovných úlohách. Používatelia pracovných rolí opísaných v pôvodnom NIST SP 800-181 ich môžu naďalej používať. Aktualizácie predchádzajúcich dokumentov môže NICE v budúcnosti zverejniť. [2]

Vzťahy medzi úlohami, znalosťami, zručnosťami a schopnosťami boli zmenené. Definície zručností a schopností z predchádzajúcej verzie boli revidované za účelom zjednodušenia do definícií zručností, ktoré sa zameriavajú na činnosť aktéra. Táto verzia popisuje metódy na priradenie definícií o znalostiach a zručnostiach k úlohám pre rôzne požadované výstupy. Zoznamy úloh, znalostí, zručností a pracovných rolí, ktoré boli predtým k dispozícii v prílohách A a B NICE koncepcie z roku 2017, boli z tejto verzie odstránené z dôvodu zjednodušenia aktualizácie NICE koncepcie a aktualizácie týchto zoznamov. Zoznam úloh, znalostí a zručností a zodpovedajúce kompetencie a pracovné úlohy budú zachované ako samostatné artefakty a budú predmetom priebežnej revízie a aktualizácie v súlade s definovaným procesom úprav a pravidlami pre verziovanie dokumentu. Pokiaľ nebudú k dispozícii aktualizované verzie, staršie verzie týchto zoznamov zostanú používateľom k dispozícii v centre rámcových zdrojov NICE. Na podporu interoperability a modularity zabezpečia budúce aktualizácie súlad definícií s definíciami úloh, znalostí a zručností uvedených v tomto dokumente.

- Pre čitateľov, ktorí majú záujem o porovnávacie štandardy, odkazy alebo zdroje pre NICE koncepciu, spolupracuje NICE v rámci programu Online Informative References (OLIR) na vývoji šablón pre vzájomné prepojenie. Program OLIR, ktorý spravuje NIST, poskytuje mechanizmus na zosúladenie odkazov na dokumenty NIST vrátane katalógu týchto odkazov. [3]

Manažérske zhrnutie

Každý z nás vykonáva individuálne a organizačne dôležitú prácu, ktorá prispieva spoločnosti. Informácie a technológie, vrátane mnohých nových typov prevádzkových technológií sú však čoraz zložitejšie a vzájomne prepojené. Je teda ťažké jasne opísať prácu, ktorá sa vykonáva alebo ktorú chceme vykonať, najmä v týchto rýchlo sa rozvíjajúcich oblastiach. Národná iniciatíva pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE) vychádza z predpokladu, že študenti, uchádzači o zamestnanie a zamestnanci v oblasti kybernetickej bezpečnosti patria medzi kontinuálne sa vzdelávajúce osoby z dôvodu neustálych zmien a nových výziev. Uvedená kategória osôb je v dokumente uvádzaná ako „aktéri“, prípadne ako „odborníci v oblasti kybernetickej bezpečnosti“ napriek tomu, že koncepcia NICE nie je určená iba pre oblasť vzdelávania sa osôb priamo pracujúcich v oblasti kybernetickej bezpečnosti. Úlohy, ktoré spadajú do pracovnej náplne pre oblasť kybernetickej bezpečnosti sú označované ako „práca v oblasti kybernetickej bezpečnosti“ a koncepcia NICE definuje spôsob, ako detailne popísať pracovné činnosti pre potreby vzdelávania a odbornej prípravy študentov, definovania pracovnej pozície pre záujemcov o prácu a pre rozvoj a vzdelávanie zamestnancov. Koncepcia NICE je vytvorená s cieľom poskytnúť referenčnú taxonómiu, to znamená definovať spoločný jazyk pre oblasť kybernetickej bezpečnosti a jednotlivých jej aktérov. Koncepcia podporuje úlohu NICE, ktorou je podpora a koordinácia veľkej skupiny odborníkov spoločne sa podieľajúcich na rozvoji integrovaného ekosystému vzdelávania v kybernetickej bezpečnosti a podpore rozvoja zamestnaneckých zručností a znalostí. Základom koncepcie NICE je skupina modulov pre popis úloh, zručností a znalostí, ktoré sú potrebné pre zvládnutie každodennej práce jednotlivcami alebo tímami. Na základe definovaných modulov poskytuje koncepcia organizáciám možnosť pre rozvoj zamestnancov a študentom pre prípravu na prácu v oblasti kybernetickej bezpečnosti vrátane možnosti zapojenia sa do vhodných vzdelávacích aktivít. Uvedený prístup pomáha zamestnávateľom a zamestnancom definovať kariérny rast na základe stanovených úloh, znalostí a zručností podľa zvoleného kompetenčného rámca.

Zavedenie spoločných pojmov a jazyka pomáha organizovať a komunikovať prácu a definovať atribúty tých, ktorí sú kvalifikovaní na vykonávanie tejto práce. NICE koncepcia týmto spôsobom pomáha zjednodušiť komunikáciu a zamerať sa na aktuálne stanovené úlohy. Použitie koncepcie NICE zvyšuje zrozumiteľnosť komunikácie na všetkých úrovniach riadenia, či už ide o jednotlivca, organizáciu, sektor alebo krajinu.

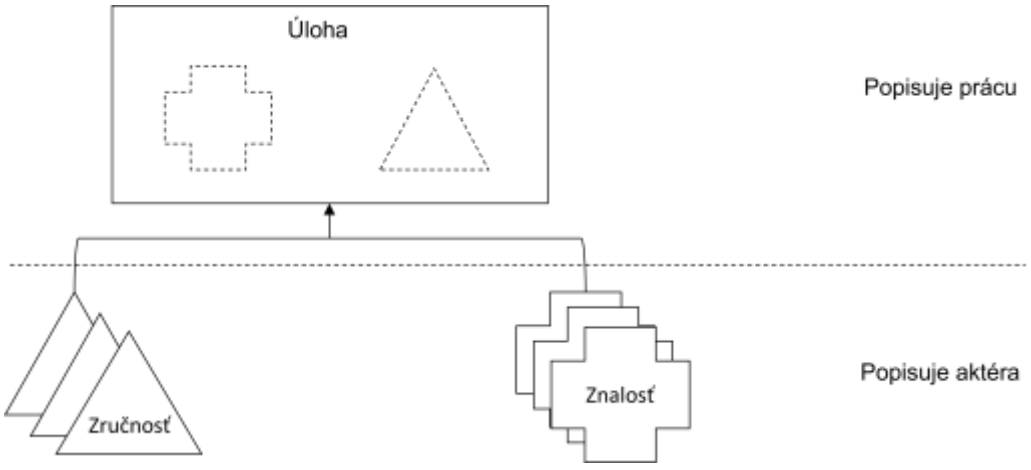
Obsah

1 Úvod

Technológie sa neustále vyvíjajú, pričom tempo zmien je veľmi vysoké. Konkrétne technológie pre spracovanie a prístup k informáciám podliehajú dramatickým zmenám. Činnosti smerujúce k návrhu, vytváraniu, zabezpečeniu a implementácii úložísk dát, sietí pre výmenu informácií a samotných informačných systémov sú čoraz komplikovanejšie a komplexnejšie. Okrem toho je samotný popis týchto činností a súvisiacich ľudských zdrojov samostatným problémom. Nezanedbateľným faktorom zvyšujúcim celkovú zložitosť daného problému je tiež rôzny prístup organizácií k jeho riešeniu.

Táto publikácia z Národnej iniciatívy pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE) popisuje koncepciu vzdelávania pre oblasť kybernetickej bezpečnosti (NICE koncepcia). Koncepcia NICE pomáha organizáciám prekonať problém opisu svojich požiadaviek na zamestnancov viacerým zainteresovaným stranám tým, že prezentuje prístup k základným modulom vzdelávania v oblasti kybernetickej bezpečnosti. NICE koncepcia zavádza prostredníctvom koncepčných modulov spoločný jazyk pre organizácie, ktorý môžu používať v rámci organizácie, ale aj pri komunikácií a s externými subjektami. Tento prístup umožňuje organizáciám prispôsobiť a implementovať NICE koncepciu na základe svojho špecifického prevádzkového kontextu. Vytvorením spoločného jazyka sa okrem toho eliminuje problém zapojenia ďalších subjektov do spolupráce.

Na obrázku 1, uvedenom nižšie, je znázornený celkový pohľad na koncepciu NICE. Hlavnými stavebnými blokmi koncepcie NICE sú popisy úloh, vedomostí a zručností (podrobne vysvetlené v Kapitole 2), ktoré sú uvedené spolu s popisovanými oblasťami. Obrázok 1 ukazuje, že sú definované dva hlavné typy pojmov: "práca" a "aktér". Tí, ktorí vykonávajú (alebo budú) vykonávať prácu (napr. študenti, súčasní zamestnanci alebo uchádzači o zamestnanie), sa neustále vzdelávajú a možno ich nájsť v ktorejkoľvek časti vzdelávacieho cyklu. Koncepcia NICE sa snaží definovať "prácu" a "aktéra" vo všeobecných termínoch, ktoré možno aplikovať na všetky organizácie.



Obrázok 1 – Celkový pohľad na NICE koncepciu

„Práca“ je činnosť potrebná na dosiahnutie cieľov v oblasti kybernetickej bezpečnosti pre elimináciu definovaných rizík. V každej organizácii existujú bežné činnosti, ktoré je možné nájsť

aj v ďalších organizáciách, ako aj činnosti, ktoré sú pre konkrétnu organizáciu špecifické. Príkladom sú štandardné manažérske úlohy, medzi špecifické úlohy potom patria úlohy typu „bezpečné nasadenie energetického systému“. NICE koncepcia poskytuje organizáciám spôsob, akým opísať prácu definíciou úloh, ktoré vychádzajú z definovaného prehľadu znalostí a zručností.

„Aktér“ je osoba, ktorá má znalosti a zručnosti. Pojem *aktér* je použitý pre všetky osoby uvádzané v tomto dokumente. Aktérom môže byť klasický študent, záujemca o prácu, zamestnanec alebo iná osoba. V kontexte organizácie je aktér zodpovedný za vykonávanie úloh. V kontexte vzdelávania získava aktér znalosti a zručnosti. Všetky osoby sú považované za aktérov z dôvodu existencie predchádzajúcich znalostí a zručností, znalostí a zručností získaných ďalším vzdelávaním, individuálnym vzdelávaním alebo skúsenosťami v priebehu kariérneho rastu.

NICE koncepcia ponúka organizáciám spôsob, ako popísať znalosti a zručnosti jednotlivca alebo skupiny. Použitím definovaných znalostí a zručností môžu osoby vykonávať úlohy smerujúce k dosiahnutiu cieľov organizácie. Napriek tomu, že organizácia nemusí aplikovať všetky koncepty NICE koncepcie týkajúce sa aktérov, poskytuje táto koncepcia flexibilnú sadu modulov pre definovanie potrieb príslušnej organizácie. Zadefinovanie roly, ktorú aktér zohráva v procese rozvoja kompetencií organizácie v oblasti kybernetickej bezpečnosti tiež zvyšuje použiteľnosť NICE koncepcie v procese vzdelávania a odbornej prípravy.

Popisom základných elementov, práce a aktéra, poskytuje NICE koncepcia organizáciám spoločný jazyk na popis práce a kompetencií v oblasti kybernetickej bezpečnosti. Časti koncepcie NICE definujú organizačný koncept práce (úlohy), vzdelávací kontext (znalosti a zručnosti), ako aj možnosť prepojenia oboch definovaných kontextov pomocou modulov NICE koncepcie.

NICE koncepcia okrem toho poskytuje mechanizmus na komunikáciu medzi organizáciami na úrovni partnerov, sektorov, štátu alebo na medzinárodnej úrovni pomocou definovaných koncepčných celkov. Táto komunikácia môže viesť k inovatívnym riešeniam spoločných problémov a zlepšeniu prístupu organizácie a osôb k zdrojom na trhu práce.

1.1 Atribúty NICE koncepcie

NICE koncepcia predstavuje referenčný zdroj informácií pre tých, ktorí potrebujú popísať prácu v oblasti kybernetickej bezpečnosti svojej organizácie a potrebné kroky pre ďalšie vzdelávanie, s cieľom dosiahnutia efektívnej práce zamestnancov v oblasti kybernetickej bezpečnosti. Charakter práce, a teda aj pracovnej sily, možno opísať pomocou stavebných blokov (znalosti, zručnosti, schopnosti) uvedených v nasledujúcich častiach.

Tieto stavebné bloky definujú nasledovné atribúty:

- **Agilnosť –** ľudia, procesy a technológie podliehajú neustálym zmenám. NICE koncepcia poskytuje nástroj pre popis neustále sa meniaceho ekosystému organizácie.
- **Flexibilita –** zatiaľ, čo každá organizácia čelí podobným výzvam, neexistuje univerzálne riešenie týchto spoločných výziev. Koncepcia NICE preto umožňuje organizáciám zohľadniť jedinečný prevádzkový kontext organizácie.

- **Interoperabilita -** napriek tomu, že každá úloha má unikátne riešenie, tieto riešenia musia byť konzistentné v rámci používania pojmov. Koncepcia NICE preto umožňuje organizáciám vymieňať si informácie o kompetenciách pomocou spoločného jazyka.

- **Modularita –** aj keď sú základom tohto dokumentu riziká v oblasti kybernetickej bezpečnosti, existujú aj ďalšie hrozby, ktorým musí organizácia čeliť. NICE koncepcia preto umožňuje organizáciám komunikovať o iných typoch kompetencii v rámci podniku, naprieč organizáciami alebo sektormi. Patrí sem napríklad ochrana súkromia, manažment rizík, či softvérové inžinierstvo.

1.2 Účel a použitie

Organizácie vykonávajú veľké množstvo pracovných činností na rôznych oddeleniach (napríklad výroba, mzdové a právne oddelenie, či oddelenie pre ľudské zdroje) ako súčasť svojej podnikateľskej činnosti. Každá z týchto činností so sebou nesie súvisiace riziká. Keďže sa technológie ako také stali podporným nástrojom pri riadení podniku, riziká spojené s kybernetickou bezpečnosťou vzrástli. Koncepcia NICE pomáha organizáciám pri riadení rizík v oblasti kybernetickej bezpečnosti tým, že poskytuje spôsob, ako diskutovať o práci a vzdelávaní v oblasti kybernetickej bezpečnosti. Tieto riziká súvisiace s kybernetickou bezpečnosťou sú dôležitým vstupom rozhodovania o podnikových rizikách, tak ako je to opísané v Medzi-agentúrnej správe NIST 8286, *Integrácia kybernetickej bezpečnosti a riadenia podnikových rizík (angl. Integrating Cybersecurity and Enterprise Risk Management, ERM).*[4]

Tento dokument slúži aj ako potenciálny sprievodca pre ďalšie pracovné činnosti, v rámci ktorých sa zvažuje vytvorenie kompetenčného rámca. Organizácie môžu zvýšiť efektivitu pomocou rovnakých stavebných blokov použitých pre rôzne pracovné činnosti, na základe čoho je tento dokument využiteľný ľubovoľnou organizáciou.

1.3 Cieľová skupina

Oblasť riadenia kompetencii pre kybernetickú bezpečnosť zahŕňa mnoho rôznych typov pozícií, ako aj mnoho rôznych typov organizácií. Cieľovou skupinou tohto dokumentu sú agentúry verejného sektora, súkromné a neziskové organizácie, vzdelávacie a tréningové inštitúcie, tvorcov učebných osnov, poskytovateľov prístupových údajov a poverení, odborníkov z oblasti ľudských zdrojov, náborových pracovníkov aj manažérov, manažérov výroby, tvorcov kompetencií a všetkých aktérov.

1.4 Členenie publikácie

Členenie tejto publikácie je nasledovné:

- Kapitola 2, Stavebné bloky koncepcie NICE, definuje komponenty NICE koncepcie v podobe blokov znalostí, zručností a schopností.

- Kapitola 3, Použitie NICE koncepcie, popisuje spoločné prístupy k používaniu NICE koncepcie.

- Kapitola 4, Záver.

- Literatúra, zoznam literatúry.
- Príloha A, Použité skratky, zoznam skratiek použitých v tejto publikácii.
- Príloha B, Slovník pojmov, vysvetlenie pojmov použitých v tejto publikácii.

2 Stavebné bloky koncepcie NICE

Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia) je založený na súbore oddelených stavebných blokov, ktoré opisujú činnosti (prácu) vykonávané vo forme úloh a kompetencie v podobe znalostí a zručností potrebných na ich vykonávanie. Tieto stavebné bloky tvoria štruktúry, ktoré podporujú použiteľnosť a implementáciu NICE koncepcie. Zároveň poskytujú mechanizmus, pomocou ktorého môžu organizácie a jednotlivci pochopiť rozsah a obsah NICE koncepcie. Stavebné bloky sú definované ako návod, ktorý možno použiť na zlepšenie porozumenia, nie na tvorbu nemenných striktných postupov.

2.1 Definície úloh

Úloha
Činnosť zameraná na dosiahnutie definovaných cieľov.

Definície úloh
- Ľahko pochopiteľné a zrozumiteľné
- Začínajú aktuálne vykonávanou činnosťou
- Neobsahujú cieľ úlohy

Ako bolo uvedené na Obrázku 1, definície úloh popisujú prácu, zatiaľ čo definície znalostí a zručností osobu, ktorá bude úlohu vykonávať. Definície úloh by mali byť zamerané na organizačný jazyk a komunikačné zvyklosti, ktoré poskytujú pridanú hodnotu pre organizáciu. Definície sú navrhnuté tak, aby popisovali prácu, ktorá sa má vykonať a mali by byť zosúladené s kontextom organizácie.

Úlohy popisujú prácu, ktorá má byť vykonaná. Úloha môže byť definovaná ako činnosť, ktorá je zameraná na dosiahnutie organizačných cieľov vrátane obchodných cieľov, technologických cieľov alebo cieľov misie. Definície úloh by mali byť jednoduché. Zatiaľ čo práca definovaná v zadaní úlohy môže mať viac krokov tak, ako je uvedené v príklade nižšie, samotná jej definícia je ľahko pochopiteľná a zrozumiteľná.

Zadanie úlohy začína činnosťou, ktorá sa bude vykonávať.

> Príklad: Riešenie problému so systémovým hardvérom a softvérom.

Definícia úlohy neobsahuje cieľ, keďže cieľ sa môže líšiť v závislosti od aktuálneho procesu a potrieb organizácie.

> Príklad: Realizovať interaktívne školenie (tréning).

Vo vyššie uvedenom príklade môže byť cieľom vytvorenie efektívneho vzdelávacieho prostredia, ale tento cieľ nie je zahrnutý v samotnej definícii úlohy.

Z Obrázok 11 vyplýva, že úlohy súvisia s definíciami znalostí a zručností. Aktér buď preukáže, že má znalosti a zručnosti na dokončenie úlohy, alebo bude vyzvaný, aby si znalosti a zručnosti doplnil a pripravil sa na realizáciu úlohy. Zložitosť úlohy je definovaná doplnkovými informáciami o znalostiach a zručnostiach. Vo vyššie uvedenom príklade s riešením systémových problémov je potrebné pre ich efektívne vyriešenie disponovať príslušnými znalosťami. To isté platí o zručnostiach.

2.2 Definície znalostí

Znalosť
Vedomosť získaná na základe štúdia alebo skúsenosti.

Definície znalostí
- Popisujú základné alebo špecifické znalosti
- Na splnenie úlohy môže byť potrebných viacero definovaných znalostí
- Na splnenie rôznych úloh je možné použiť rovnakú znalosť

Definície znalostí sú úzko prepojené s definíciami úloh, pretože iba v prípade disponovania danou znalosťou je možné úlohu splniť. Znalosti sú definované ako opakovane použiteľné vedomosti získané na základe štúdia alebo skúsenosti. Definície znalostí môžu popisovať základné alebo špecifické koncepty. Na splnenie danej úlohy môže byť potrebných viacero znalostí, podobne je možné jednu znalosť použiť na splnenie viacerých úloh.

Definície znalostí môžu byť jednoduché (základné).

> Príklad: Znalosť kybernetických hrozieb a zraniteľností.

Príklad špecifickej znalosti je uvedený nižšie.

> Príklad: Znalosti o zraniteľnosti zdrojov šírenia informácií (napr. upozornenia dodávateľov, vládne poradenstvo, tlačové chyby v produktových materiáloch a bulletinoch).

Organizácie, ktoré vytvárajú definície znalostí, by mali zvážiť rôzne úrovne vedomostí a odborných znalostí aktérov. Príklad takýchto rôznych úrovní je popísaný v Bloomovej taxonómii (revidovaná edícia), ktorá používa jazyk na uľahčenie posúdenia a ohodnotenia aktéra. [5]

2.3 Definície zručností

Zručnosť
Schopnosť vykonať pozorovateľnú činnosť.

Definície zručností
- Popisujú jednoduché alebo zložité zručnosti
- Na splnenie úlohy môže byť potrebných viacero zručností
- Na splnenie rôznych úloh je možné použiť rovnakú zručnosť

Definície zručností sú úzko prepojené s definíciami úloh, pretože aktér potrebuje zručnosti pri vykonávaní úloh. Aktér, ktorý nie je schopný použiť definovanú zručnosť, nebude schopný splniť úlohu, ktorá je na túto zručnosť naviazaná. Zručnosť je definovaná ako schopnosť vykonať pozorovateľnú činnosť. Definície zručností môžu opisovať jednoduché alebo zložité zručnosti. Niekedy je potrebné na splnenie danej úlohy ovládať viaceré zručnosti, podobne môže byť jedna zručnosť použitá na splnenie viacerých úloh.

Definície zručností môžu byť jednoduché.

> Príklad: Zručnosť pri rozpoznávaní upozornení zo systému na detekciu prieniku (angl. Intrusion Detection System).

Príklad zložitej zručnosti je uvedený nižšie.

> Príklad: Zručnosť pre vytváranie hypotézy o tom, ako aktér hrozby obišiel systém detekcie prieniku.

Ako je znázornené na Obrázku 1, definície zručností popisujú, čo môže aktér urobiť. Definície úloh popisujú prácu, ktorú je potrebné vykonať. Je preto potrebné oddeliť jazyk používaný

v definíciách zručností od jazyka používaného v definíciách úloh a používať výrazy, ktoré uľahčujú posúdenie a hodnotenie aktéra.

3 Použitie NICE koncepcie

Napriek tomu, že Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia) poskytuje spoločnú množinu elementov (stavebných blokov), ktoré je možné priamo použiť, je pre niektoré organizácie nevyhnutné prispôsobiť si model tak, aby bol lepšie zosúladený s ich jedinečným kontextom. Výrobný podnik môže mať napríklad definované špecifické úlohy pre jeho odvetvie alebo organizáciu, ktoré nie sú popísané v NICE koncepcii. Je tiež možné dôjsť k záveru, že definície úloh sú aplikovateľné, ale musia byť upravené alebo doplnené o konkrétne definície znalostí a zručností s cieľom realizovateľnosti úloh definovaných v ich jedinečnom kontexte. Jednotlivé stavebné bloky nie sú teda pevne dané, ale predstavujú spoločný jazyk pre organizácie alebo odvetvia na použitie takým spôsobom, ktorý je výhodný pre dané prostredie.

Príklady použitia stavebných blokov koncepcie NICE, uvedené nižšie, majú teoretický resp. koncepčný charakter. Organizácia môže používať stavebné bloky akýmkoľvek spôsobom, ktorý najlepšie vyhovuje jej potrebám. Zobrazené príklady sú určené na ilustráciu potenciálnych praktických prístupov k NICE koncepcii a slúžia ako pomoc pre dosiahnutie spoločných cieľov organizácie. Poskytujú organizáciám alebo odvetviam návod v prípade, že chcú aplikovať nový bezpečnostný koncept.

3.1 Použitie existujúcich definícií úloh, znalostí a zručností

Používatelia NICE koncepcie odkazujú na jednu alebo viacero definícií úloh, znalostí a zručností tak, ako je popísané v Kapitole 2 pre popis práce a aktérov. Definície úloh sú použité na opis práce a spájajú definície znalostí a zručností. Aj keď môže mať definícia úlohy odporúčanú množinu definovaných znalostí a zručností, môžu používatelia úlohe priradiť aj iné existujúce definície znalostí a zručností pre prispôsobenie úlohy jej jedinečnému kontextu. Definície znalostí a zručností sa používajú na popis aktérov a môžu byť použité rôznymi spôsobmi na riadenie ľudských zdrojov pre oblasť kybernetickej bezpečnosti. Môžu byť použité ako celok, časť, resp. nemusia byť použité vôbec s ohľadom na unikátny charakter organizácie. Definície úloh, znalostí a zručností môžu byť použité:

- V rámci programu pre sledovanie zručností na určenie kvalifikačných predpokladov kariérneho postupu.
- Na stanovenie znalostí potrebných pre absolvovanie kurzu.
- Na definíciu týždenných úloh, ktoré je potrebné vykonať v organizácii.

Definície úloh, znalostí a zručností je možné nájsť na stránke zdrojov NICE koncepcie (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center). Definície sú aktualizované na základe potrieb a nových požiadaviek tak, aby reflektovali aktuálny stav poznania a technológie. [1]

3.2 Vytváranie nových definícií znalostí a zručností

Používatelia by nemali upravovať text existujúcich definícií úloh, znalostí a zručností NICE koncepcie. Vytvorené definície sú určené na podporu interoperability, takže zmena ich obsahu môže mať za následok následné nezrovnalosti pri používaní externými spolupracujúcimi entitami.

Ak je potrebné vytvoriť iné znenie definície z dôvodu podpory jedinečného kontextu používateľa, je možné vytvoriť novú definíciu.

Používatelia majú možnosť vytvoriť úplne novú definíciu úlohy, znalosti alebo zručnosti, ktorou umožnia prispôsobenie NICE koncepcie pre použitie v rámci ich jedinečného kontextu. Takéto dodatočné definície pomôžu podporiť jasné a konzistentné interné prostredie týkajúce sa aktérov a ich pracovných činností.

3.3 Kompetencie

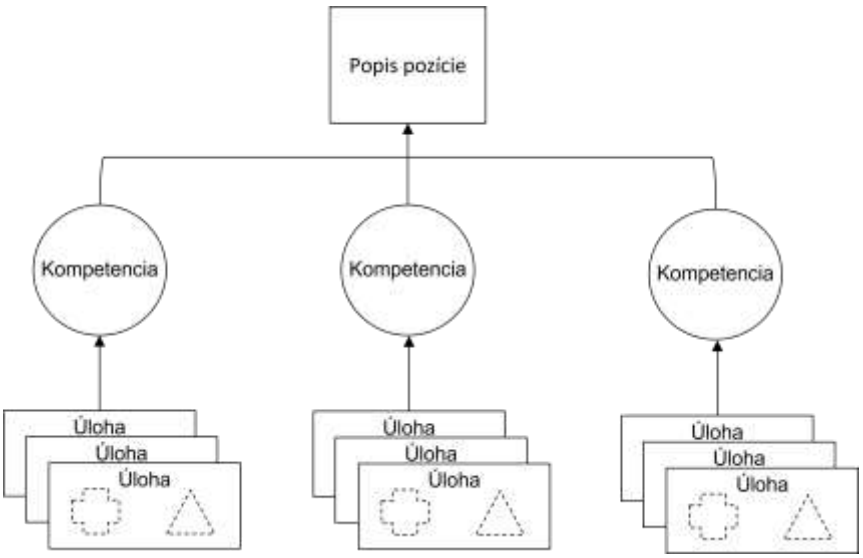
Kompetencie poskytujú organizáciám mechanizmus na posudzovanie aktérov. Sú definované prostredníctvom zamestnávateľom riadeného prístupu, ktorý poskytuje prehľad o jedinečnom kontexte organizácie. Okrem toho umožňujú kompetencie poskytovateľom vzdelávania a odbornej prípravy reagovať na potreby zamestnávateľov alebo sektora rozvíjaním vzdelávacích zručností, ktoré pomáhajú študentom rozvíjať kompetencie. Definícia kompetencie pozostáva z názvu, opisu kompetencie, hodnotiacej metódy, ako aj skupiny súvisiacich definícií úloh, znalostí a zručností.

Kompetencia
Je mechanizmus na ohodnotenie odbornosti aktérov organizáciou.

Kompetencie sú
- Definované na základe zamestnávateľom riadeného prístupu
- Zamerané na aktérov
- Pozorovateľné a merateľné

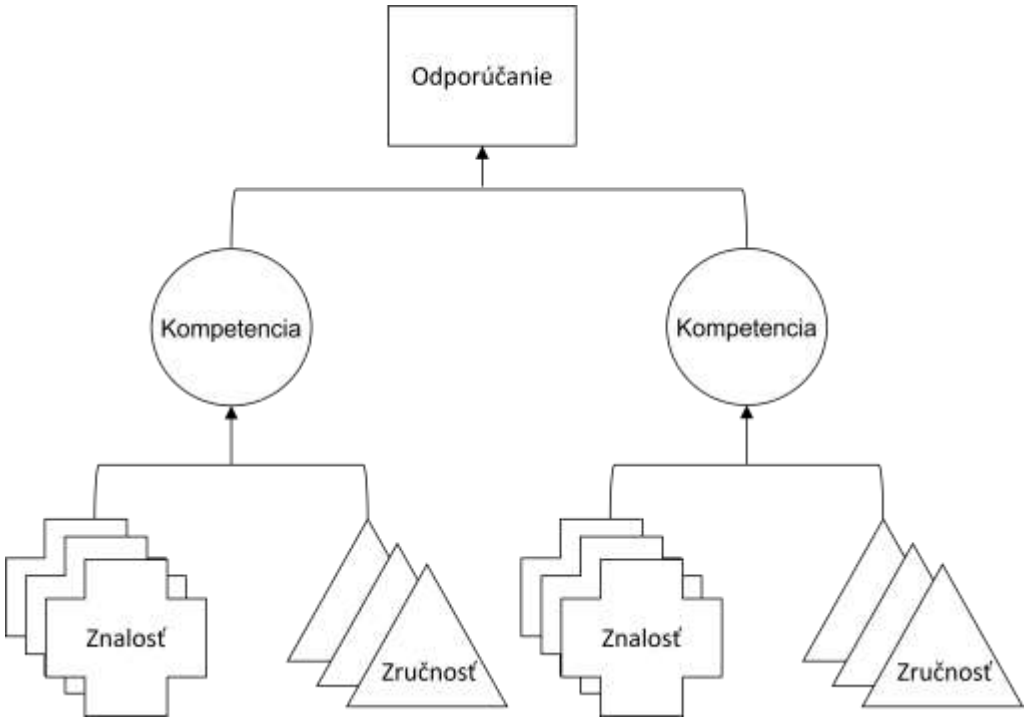
Kompetencie poskytujú flexibilitu tým, že umožňujú organizáciám zoskupiť rôzne definície úloh, znalostí a zručností do jednej zastrešujúcej kategórie, ktorá definuje širokú paletu potrieb. Zatiaľ čo konkrétna úloha a jej súvisiace definície o znalostiach a zručnostiach sa nemusia meniť, širšie definovaná kompetencia môže zaviesť nové úlohy alebo dokonca jednotlivé znalosti a zručnosti (prípadne odstrániť existujúce) v reakcii na meniace sa potreby v ekosystéme kybernetickej bezpečnosti.

Existujú rôzne spôsoby, ako používať kompetencie. Organizácia napríklad môže použiť kompetencie ako súčasť procesu prijímania zamestnancov s ohľadom na dosiahnutie stanoveného cieľa (obrázok 2). V takomto prípade je možné definovať kompetencie ako skupinu súvisiacich definícií úloh. Organizácia by potom mala kompetencie používať na posúdenie, či je daný kandidát schopný tieto úlohy vykonať. Hodnotenie by malo mať formu pohovoru, testu alebo vyhodnotenia výsledkov vzdelávania pred samotným zamestnaním uchádzača.



Obrázok 2. Použitie kompetencií na hodnotenie uchádzačov pomocou popisu pozície

Iné organizácie by mohli využívať kompetencie na určenie, či aktér dosiahol definovaný súbor zručností a vedomostí. Takéto organizácie môžu použiť kompetencie ako skupiny definícií znalostí a zručností (obrázok 3) na posúdenie schopností uchádzača. Hodnotenie by malo mať formu testu, praktického zadania alebo ústnych hodnotení.



Obrázok 3. Použitie kompetencií na hodnotenie uchádzačov pomocou odporúčaní

Vyššie uvedené príklady sú ukážkou použitia kompetencií, pričom môžu byť použité ako celok alebo čiastočne v závislosti od jedinečného kontextu implementujúcej organizácie.

3.3.1 Použitie existujúcich kompetencií

Kompetencie NICE koncepcie sú pre organizácie spôsobom, ako sa zosúladiť s NICE koncepciou na všeobecnej úrovni bez nutnosti podrobne sa zaoberať definíciami úloh, znalostí a zručností. Kompetencie tvoria spôsob, ako opísať aktéra. Definovaním skupín úloh, znalostí a zručností majú organizácie možnosť jednoducho definovať kompetencie, komunikovať a efektívne organizovať prácu v oblasti kybernetickej bezpečnosti a získať zjednodušený pohľad na pracovnú silu. Kompetencie je možné ďalej využiť na :

- Popis typov úloh na danej pozícii.
- Sledovanie schopností pracovníkov.
- Opis požiadaviek na pracovnú skupinu.
- Preukázanie schopností aktérov.

Hoci majú kompetencie odporúčanú množinu definovaných úloh, znalostí a zručností, používatelia majú možnosť pridať alebo odobrať novú definíciu na prispôsobenie kompetencií svojmu unikátnemu kontextu. Používatelia sú však varovaní pred zmenou názvu alebo popisu existujúcich kompetencií definovaných NICE koncepciou. Kompetencie sú určené na podporu interoperability, takže zmena ich obsahu môže mať za následok následné nezrovnalosti pri používaní externými entitami. Ak je v kompetencii potrebné iné znenie na podporu jedinečného kontextu používateľa, môže sa vytvoriť nová kompetencia tak, ako je opísané nižšie (pozri časť 3.3.2).

3.3.2 Vytváranie nových kompetencií

Pre niektoré organizácie môže byť žiadúce definovať kompetenciu pre konkrétny kontext svojej práce v oblasti kybernetickej bezpečnosti. NICE koncepcia je vytvorená na základe agilných princípov a umožňuje organizáciám definovať kompetenciu na základe požiadaviek meniaceho sa ekosystému kybernetickej bezpečnosti. Toto je možné dosiahnuť zmenou existujúcej kompetencie v súlade s aktuálnymi potrebami alebo vytvorením úplne novej kompetencie.

Dva nižšie uvedené príklady slúžia na vysvetlenie potenciálnych procesov pri používaní kompetencií. Tieto dva príklady sa zameriavajú na analýzu dát, aby ukázali, že rovnaká kompetencia môže byť použitá prostredníctvom rôznych prístupov. Tieto príklady sú rozpracované na Obrázok 2 a Obrázok 3 aby čitateľovi bola objasnená ich potenciálna implementácia. Príklady sú uvedené vo forme tabuľky na komunikáciu kompetencie. Tento tabuľkový prístup je jedným z mnohých, ktoré môže organizácia pri implementácii kompetencie použiť.

Analýza dát – príklad 1

Tabuľka 1, uvedená nižšie, je informatívna a poskytuje východiskový bod pre tvorbu kompetencie. Kompetencia v príklade analýzy dát má svoj názov a popis, ktorým je možná jej rýchla identifikácia organizáciou ako kompetencie, ktorá má hodnotu pre jej organizačnú štruktúru a kontext. Pomocou metódy hodnotenia praktickej činnosti organizácia hodnotí aktéra tým, že

poskytuje simulované pracovné prostredie na realizáciu úloh, ktoré spĺňajú ich procesné ciele. (Tabuľka Tabuľka 1[2]

Tabuľka 1 – Príklad vytvorenia novej kompetencie pre analýzu dát pomocou existujúcej NICE koncepcie z roku 2017

Názov kompetencie: Analýza dát – príklad 1
Popis kompetencie: Zber**,** syntéza alebo analýza kvalitatívnych a kvantitatívnych dát a informácií z rôznych zdrojov na podporu rozhodovania, vypracovanie odporúčaní a/alebo tvorbu reportov, zhrnutí a dokumentácie.
Spôsob hodnotenia: Praktické cvičenie
Definície úloh
T0007 | Analyzujte a definujte požiadavky na dáta a ich špecifikáciu.
T0405 | Použite Open Source jazyk, ako napríklad jazyk R a aplikujte kvantitatívne techniky (napr. deskriptívnu a inferenčnú štatistiku, vzorkovanie, návrh experimentov, parametrické a neparametrické testy rozdielnosti, metódu najmenších štvorcov, regresiu).

V príklade uvedenom v Tabuľka 1 môže organizácia poskytnúť aktérovi počítač, ktorý obsahuje konkrétnu množinu dát a je pripojený k laboratórnej sieti. Aktérovi sa následne poskytne čas, počas ktorého má preukázať svoju schopnosť používať Open Source jazyky na aplikovanie kvantitatívnych techník pre spracovanie dát. Kľúčovou časťou tohto hodnotenia je analýza dát, ktorá zabezpečí, že dáta spĺňajú konkrétnu špecifikáciu dát pred dokončením samotnej analýzy. Prostredníctvom tohto hodnotenia aktér preukazuje kompetenciu "Analýza dát – príklad 1" definovanú zamestnávateľom.

Podrobná definícia kompetencie pre analýzu dát môže byť ďaleko rozsiahlejšia. Vymenovaním definícií úloh v rámci kompetencie môže organizácia špecifikovať požadovaný rozsah znalostí, zručností a schopností v rámci kompetencie. Pre jednoduché použitie sú pre popis kompetencie použité definície úloh NICE koncepcie z roku 2017.

Analýza dát – príklad 2

Nižšie uvedená Tabuľka 2 ukazuje ďalší východiskový krok pre vytvorenie kompetencie. Príklad je znova informatívny, popis je rovnaký ako v tabuľke Tabuľka 1 pričom tento príklad používa definície znalostí a zručností na definovanie kompetencie.

Tabuľka 2 – Príklad vytvorenia novej kompetencie pre analýzu dát pomocou definície znalostí a zručností

Názov kompetencie: Analýza dát – príklad 2
Popis kompetencie: Zber**,** syntéza alebo analýza kvalitatívnych a kvantitatívnych dát a informácií z rôznych zdrojov na podporu rozhodovania, vypracovanie odporúčaní a/alebo tvorbu reportov, zhrnutí a dokumentácie.
Spôsob hodnotenia: test

Definície znalostí a zručností
S0013 | Zručnosť vo vytváraní databázových dotazov, vývoji algoritmov a analýze dátových štruktúr.
S0021 | Zručnosť pri navrhovaní štruktúr pre analýzu dát (napr. dátových typov, ktoré musí test generovať a postupov pre analýzu dát).
S0091 | Zručnosť pre analýzu neurčitých dát.
K0020 | Znalosť administrácie dát a dátových štandardov.
K0338 | Znalosť dataminingových techník.

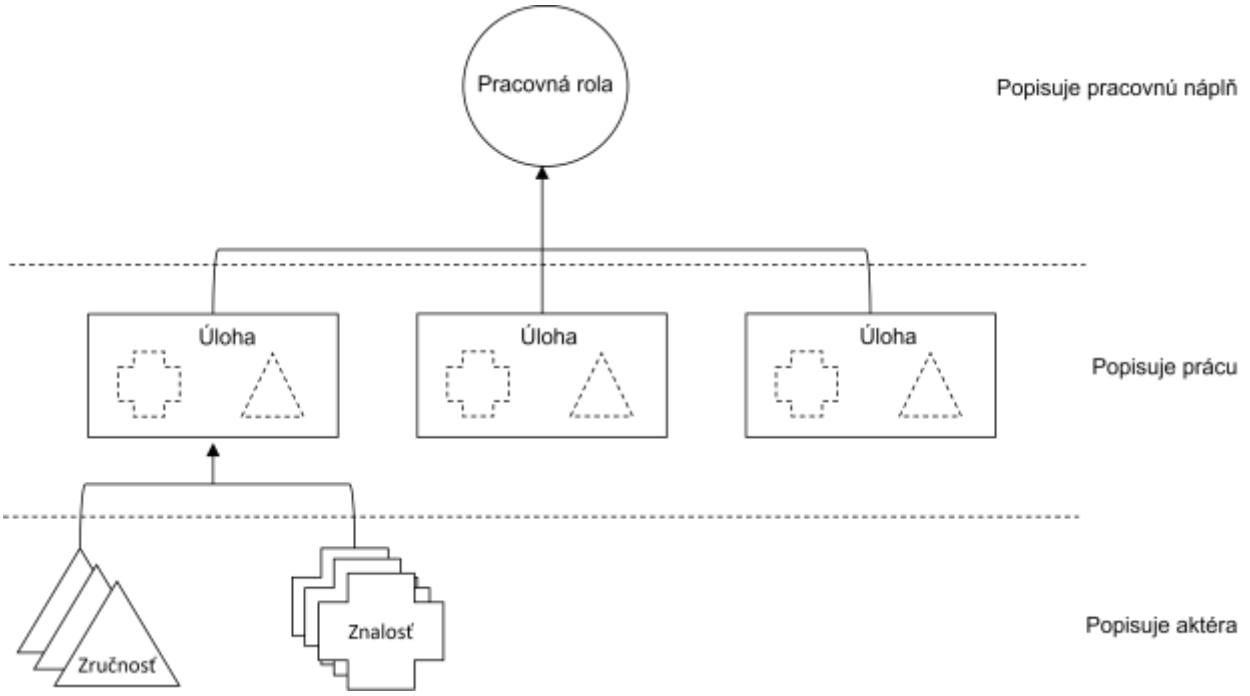
V tomto príklade predstavuje Tabuľka 2 kompetenciu pre analýzu dát. Túto kompetenciu môže vytvoriť testovacia / vzdelávacia autorita, ktorá poskytuje test na hodnotenie aktérov. Test môže byť realizovaný v papierovej alebo elektronickej forme prostredníctvom počítačov. Absolvovaním testu aktér preukáže kompetenciu "Analýza dát – príklad 2" definovanú testovacou autoritou.

(Poznámka: V Tabuľka 2 sú použité definície znalostí a zručností verzie NICE koncepcie z roku 2017. [2])

3.4 Roly

Pracovné roly sú bežným prípadom použitia koncepcie NICE. Pracovné roly sú spôsob, ako opísať zoskupenie práce, za ktorú je niekto zodpovedný.

Zatiaľ čo predchádzajúce rámce tiež spájali pracovné roly so špecifickými znalosťami, zručnosťami a schopnosťami, rámec NICE podporuje agilnejší prístup prostredníctvom úloh. Pracovné roly sa skladajú z úloh, ktoré predstavujú prácu, ktorá sa má vykonať. Úlohy zahŕňajú súvisiace definície vedomostí a zručností, ktoré predstavujú potenciál aktérov vykonávať tieto úlohy. Tento prechodný prístup, znázornený na obrázku Obrázok 4 podporuje flexibilitu a zjednodušuje komunikáciu.



Obrázok 4 – Vzťahy pracovných rolí a stavebných blokov

Názvy pracovných rolí nie sú synonymom pre názvy pracovných pozícií. Niektoré pracovné roly sa môžu zhodovať s názvom pracovnej pozície v závislosti od používania názvov pracovných pozícií organizáciou. Okrem toho tiež pracovné roly nie sú synonymom pre profesie.

Jedna pracovná rola (napr. vývojár softvéru) sa môže vzťahovať k viacerým pracovným pozíciám (napr. softvérový inžinier, programátor, vývojár aplikácií). Naopak, na vytvorenie konkrétnej pracovnej pozície sa môžu kombinovať viaceré roly. Tento doplnkový prístup podporuje lepšiu modularitu a ilustruje skutočnosť, že aktéri vykonávajú viaceré úlohy v rôznych rolách bez ohľadu na ich pracovnú pozíciu. Podobne koncepcia NICE nedefinuje úrovne odbornosti (napr. základná, stredná, pokročilá). Takéto atribúty a atribúty týkajúce sa odbornosti, s akou aktér vykonáva úlohy, sú ponechané na iné modely alebo zdroje.

3.4.1 Použitie existujúcich rolí

Každá pracovná rola je určená na podporu dosahovania cieľov prostredníctvom úloh. Hoci pracovná rola môže mať vopred určenú množinu definovaných úloh, používatelia majú možnosť zahrnúť aj iné existujúce úlohy na prispôsobenie pracovných rolí ich jedinečnému kontextu. Podobne môže používateľ chcieť čerpať z uvedených pracovných rolí alebo pridať ďalšie na podporu ďalších cieľov. Aktuálna množina komponentov NICE koncepcie je k dispozícii v NICE Framework Resource Center. [1]

Používatelia sú varovaní pred internou úpravou názvu a popisu existujúcej pracovnej roly. Pracovné roly sú určené na podporu interoperability, takže zmena ich obsahu môže viesť k následným nezrovnalostiam. Ak je potrebné iné znenie, môže sa vytvoriť nová pracovná rola, ako je popísané nižšie.

3.4.2 Vytváranie nových rolí

Používatelia môžu vytvoriť nové pracovné roly, ktoré pomôžu prispôsobiť používanie NICE koncepcie ich jedinečnému kontextu. Takéto dodatočné pracovné roly pomôžu podporiť jasné a konzistentné interné diskusie týkajúce sa práce v oblasti kybernetickej bezpečnosti.

3.5 Pracovné skupiny

Mnohé organizácie používajú pracovné skupiny (tímy) na kolektívne riešenie zložitých úloh tým, že spájajú jednotlivcov s potrebnými zručnosťami a skúsenosťami. S využitím rôznych zdrojov a perspektív je možné pomocou pracovných skupín riadiť riziká holisticky. Pracovné skupiny využívajú špecializáciu v oblasti znalostí a procesov každého člena na efektívne rozdelenie práce. Pracovné skupiny je možné definovať pomocou pracovných rolí alebo kompetencií.

3.5.1 Vytváranie pracovných skupín rolami

Prístup budovania pracovných skupín prostredníctvom rolí umožňuje organizáciám definovať, aké typy pracovných rolí sú potrebné na dosiahnutie definovaných cieľov. Keďže sa samotné pracovné roly skladajú z kompetencií, tento prístup k budovaniu pracovných skupín sa začína identifikáciou práce, ktorú treba vykonať. Tento prístup možno považovať za prístup zhora-nadol.

Tabuľka 3 -Príklad definície pracovnej skupiny pre vývoj bezpečného softvéru pomocou pracovných rolí NICE koncepcie z roku 2017

Fáza životného cyklu	Pracovná rola
Dizajn	SP-ARC-002 | Bezpečnostný architekt
Vývoj	SP-DEV-001 | Softvérový vývojár
Nasadenie	OM-NET-001 | Špecialista pre sieťové operácie
Prevádzka	OM-STS-001 | Špecialista technickej podpory
Údržba	OM-DTA-001 | Správca databázy
Odstavenie	OV-LGA-001 | Poradca pre oblasť legislatívy v kybernetickej bezpečnosti

Vyššie uvedená tabuľka 3 ukazuje spôsob vytvorenia pracovnej skupiny pre vývoj bezpečného softvéru. Pracovné roly sú vytvorené na základe identifikátorov pracovných rolí v koncepcii NICE z roku 2017. Pracovné skupiny, ktoré sú vytvárané týmto spôsobom začínajú identifikáciou práce, ktorú je potrebné vykonať. V tomto prípade je pracovná skupina pre vývoj bezpečného softvéru organizovaná fázou životného cyklu. Prvý riadok tabuľky predstavuje fázu návrhu, v ktorej pracovná skupina spolu s bezpečnostným architektom zváži ciele, vrátane plánovania. Tabuľka 3 je informatívny príklad a nepokrýva všetky pracovné roly, ktoré môžu byť vytvorené alebo potrebné pre danú pracovnú skupinu. Ďalšie informácie nájdete v dokumente *NIST's Secure Software Development Framework*. [6]

Tabuľka 4 – Príklad definície pracovnej skupiny pomocou pracovných rolí NICE koncepcie z roku 2017 a nových pracovných rolí

Funkcia koncepcie kybernetickej bezpečnosti	Pracovná rola
Identifikácia	NováPracovnáRola1 | Manažér rizík
Ochrana	SP-RSK-002 | Audítor bezpečnostného riadenia
Detekcia	PR-CDA-001 | Analytik kybernetickej obrany
Reakcia	PR-CIR-001| Respondent na incidenty kybernetickej obrany
Obnova	NováPracovnáRola2 | Špecialista komunikácie

Tabuľka 4 uvádza príklad definície pracovnej skupiny pre oblasť kybernetickej bezpečnosti. Podobne ako pracovná skupina pre vývoj bezpečného softvéru, aj tento vzorový tím je vytvorený prístupom zameraným na prácu. Použitím elementárnej časti (ang. Framework Core) *Rámca na Zlepšenie Kybernetickej Bezpečnosti Kritickej Infraštruktúry* (ang. *Framework for Improving Critical Infrastructure Cybersecurity*) sa vyberú ciele kybernetickej bezpečnosti, identifikujú sa úlohy na dosiahnutie týchto cieľov a vyberú sa pracovné roly tak, aby sa definovali úlohy potrebné na podporu týchto cieľov. [7] Tabuľka 4 je informatívny príklad a nepokrýva všetky pracovné roly, ktoré môžu byť vytvorené alebo požadované pre danú pracovnú skupinu. Boli vytvorené dve nové pracovné roly, ktoré ukazujú zmiešaný prístup používania existujúcich rolí (časť 3.4.1) a vytvárania nových rolí (časť 3.4.2). Vytvorením nových pracovných rolí demonštruje tento príklad flexibilný a agilný prístup k prispôsobeniu NICE koncepcie.

3.5.2 Vytváranie pracovných skupín kompetenciami

Pracovné skupiny je možné vytvárať aj pomocou kompetencií. Tento prístup k vytváraniu pracovných skupín pripúšťa, že jednotlivé úlohy môžu byť neznáme, ale kompetencie potrebné na vyriešenie úloh sú známe. Uvedený prístup je možné považovať za prístup zdola-nahor. Takto vytvorené pracovné skupiny môžu pomôcť identifikovať aktérov, ktorí sa môžu v budúcnosti podieľať na práci skupiny. Takýto aktéri môžu alebo nemusia byť priradení k pracovnej role a majú kompetencie potrebné na dosiahnutie cieľov organizácie.

Napríklad obranná pracovná skupina pre kybernetickú bezpečnosť, ktorá využíva svoje schopnosti na napodobňovanie techník útoku protivníkov (tzv. červený tím), môže pozostávať z nasledujúcich teoretických kompetencií:

- Plánovanie zapojenia.
- Pravidlá zapojenia.
- Penetračné testovanie.
- Forenzná analýza dát.
- Využívanie zraniteľností.

Vytvorením pracovných skupín alebo iných zoskupení znalostí a zručností si môže každá organizácia prispôsobiť NICE koncepciu spôsobom, ktorý najlepšie pomôže aplikovať a komunikovať o aktéroch a o práci, ktorú títo aktéri budú vykonávať tak, aby umožnili dosiahnutie cieľov misie.

4 Záver

Použitím prístupu, založenom na stavebných blokoch opísaných v koncepcii NICE, môžu používatelia profitovať z konzistentnej metódy organizácie a komunikácie práce, ktorá sa má vykonať, prostredníctvom výkazov úloh, vedomostí a zručností jednotlivých aktérov, ktorí túto prácu podporujú. Koncepcia NICE pomáha usmerňovať úsilie zamestnávateľov opísať prácu v oblasti kybernetickej bezpečnosti, poskytovateľov vzdelávania a školení s cieľom pripraviť pracovníkov v oblasti kybernetickej bezpečnosti a aktérov tak, aby preukázali svoje schopnosti vykonávať príslušnú prácu v oblasti kybernetickej bezpečnosti.

Možnosť popísať úlohy, vedomosti a zručnosti je dôležitá na zabezpečenie komplexného pochopenia práce a pracovnej sily. Koncepcia NICE poskytuje rozšíriteľný referenčný zdroj, ktorý je možné aplikovať a použiť rôznymi organizáciami alebo sektormi na opis práce, ktorá sa má vykonať vo viacerých oblastiach. Výhody vyplývajúce z použitia NICE koncepcie podporujú misiu NICE, ktorou je motivácia, propagácia a koordinácia silnej komunity spolupracujúcej na presadzovaní integrovaného ekosystému vzdelávania, školenia a rozvoja pracovnej sily v oblasti kybernetickej bezpečnosti.

Literatúra

[1] National Initiative for Cybersecurity Education (2020) *NICE Framework Resource Center*. Dostupné na https://www.nist.gov/nice/framework

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[3] National Institute of Standards and Technology (2020) *National Online Informative References Program*. Dostupné na https://csrc.nist.gov/projects/olir

[4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. Dostupné na https://www.depauw.edu/files/resources/krathwohl.pdf

[6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

[7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

Appendix A—Použité skratky

Vybraté skratky použité v tomto dokumente a ďalších dokumentoch NICE:

ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
ITL	NIST Information Technology Laboratory
K&S	Knowledge and Skill statement(s)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OLIR	Online Informative Reference
OMB	Office of Management and Budget
SSDF	Secure Software Development Framework
TKS	Task, Knowledge, and Skill statements

Appendix B—Slovník pojmov

Kompletný slovník pojmov v anglickom jazyku je na stránke https://csrc.nist.gov/glossary.

Kompetencia Mechanizmus na ohodnotenie odbornosti aktérov organizáciou.

Znalosť Vedomosť získaná na základe štúdia alebo skúsenosti.

Zručnosť Schopnosť vykonať pozorovateľnú činnosť.

Úloha Činnosť zameraná na dosiahnutie definovaných cieľov.