PARP
Grupa PFR

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

CYBERBEZPIECZEŃSTWO

Analiza systemów opisu kompetencji i wymagań. Rekomendacje w sprawie programów edukacyjnych dla cyberbezpieczeństwa

CELE I ADRESACI KOMPENDIUM CYBERBEZPIECZEŃSTWA

Rzeczywistość i świat, w którym funkcjonujemy, stają się cyfrowe. Przynosi to olbrzymie korzyści, ale i poważne wyzwania, wśród których największy ciężar gatunkowy ma kwestia zapewniania cyberbezpieczeństwa.

Analiza umieszczona w tej broszurze poświęcona jest pozycjonowaniu cyberbezpieczeństwa oraz istniejących systemów opisywania kompetencji i wymogów w tym zakresie. Kierujemy ją do liderek i liderów gospodarczych, w tym branży cyfrowej i cyberbezpieczeństwa. Chcielibyśmy, aby pomogła nadać odpowiednią dynamikę dyskusji o aktualnych i przyszłych wyzwaniach cyberbezpieczeństwa i przyspieszyła uzyskanie konsensusu w tej sprawie. Adresatami są też autorzy programów edukacyjnych ukierunkowanych na kształcenie specjalistek i specjalistów cyberbezpieczeństwa. Podkreślamy przy tym konieczność nieustannego obserwowania kierunków ewolucji tej dziedziny i uwzględniania zmian w programach edukacyjnych.

Podsumowaniem analizy jest zbiór rekomendacji, które wraz z opisem podstaw budowania systemów cyberbezpieczeństwa w przedsiębiorstwach i organizacjach zostały wykorzystane w osobnym poradniku cyberbezpieczeństwa. To opracowanie kierujemy do doradców edukacyjnych, uczestników i uczestniczek programów szkoleniowych w zakresie cyberbezpieczeństwa, do małych, średnich i większych firm oraz organizacji mierzących się z szybko rosnącą liczbą cyberzagrożeń. Staramy się też przygotować środowisko biznesowe na konieczność dostosowania ich organizacji do nadchodzących zmian legislacyjnych dotyczących cyberbezpieczeństwa.

Analiza wraz z rekomendacjami oraz poradnik tworzą – mamy nadzieję – całościowe Kompendium Cyberbezpieczeństwa.

STRUKTURA GRUP DOCELOWYCH KOMPENDIUM CYBERBEZPIECZEŃSTWA

Publikacja realizowana w ramach Projektu pn. „Utworzenie i funkcjonowanie Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo".
Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza, Edukacja, Rozwój.

Autorzy opracowania: **Zespół ekspercki Ośrodka THINKTANK**
Realizator publikacji: Ośrodek THINKTANK
Redaktor: Zbigniew Gajewski
Korekta: Anna Chyckowska, Małgorzata Gerasimiuk
Opracowanie graficzne: Dorota Jędrkiewicz
ISBN 978-83-967447-7-7 Warszawa 2023

SPIS TREŚCI

Uwaga redakcyjna

Z merytorycznego punktu widzenia nieodzowne było sięganie w tym opracowaniu do źródeł anglojęzycznych. Terminologia w nich stosowana nie zawsze dała się precyzyjnie przełożyć na język polski. Niemniej ponieważ zakładamy, że wśród adresatów tego opracowania są osoby na co dzień posługujące się językiem angielskim, pozostawiliśmy wiele terminów bez tłumaczenia.

1

ANALIZA SYSTEMÓW OPISU KOMPETENCJI I WYMAGAŃ W ZAKRESIE CYBERBEZPIECZEŃSTWA

WSTĘP

W większości procesów gospodarczych i społecznych, w których mają udział narzędzia informatyczne, wykładniczo rośnie rola cyberbezpieczeństwa. Trwa właśnie pospieszna cyfryzacja przedsiębiorstw, cyfryzacja usług publicznych, cyfryzacja interakcji firm z ich klientami. Dochodzi do tego cyfryzacja interakcji społecznych, wyrażająca się powszechnym wykorzystaniem mediów społecznościowych i komercyjnych mediów cyfrowych.

Dodatkowe wzmocnienie wagi tej tematyki ma swe źródło w rosnącym zaangażowaniu narzędzi cyfrowych w sferze militarnej oraz wykorzystaniu ich przez niektóre rządy do prowadzenia hybrydowych wojen cybernetycznych.

Zapewnianie cyberbezpieczeństwa ma zarówno charakter prewencyjny, jak i jest konieczne ze względu na rosnącą skalę ataków cybernetycznych i ich koszty. Według danych Komisji Europejskiej, publikowanych we wstępie uzasadniającym wprowadzenie regulacji Cyber Resilience Act, „sprzęt i oprogramowanie coraz częściej padają celem udanych cyberataków, które w 2021 r. spowodowały globalne straty w wysokości szacowanej na 5,5 bilionów EUR”[1]. Warto zaznaczyć, że nie jest to błąd tłumaczenia, w angielskiej wersji dokumentów figuruje bowiem kwota 5,5 tryliona euro. Zatem światowe straty powodowane atakami cybernetycznymi są większe niż roczne PKB Niemiec, które zbliża się do kwoty 4 bln euro.

Skala tych wyzwań i zagrożenia z nimi powiązane będą jedynie rosnąć z racji rozwoju technologii, które mogą być wykorzystywane zarówno do zwiększenia bezpieczeństwa cybernetycznego, jak i przez cyberprzestępców i wrogie państwa. Zwłaszcza narzędzia oparte na sztucznej inteligencji mogą znacząco zwiększyć rozmiar zagrożeń, ich strukturę i złożoność.

Według Midyear Cybersecurity Report 2023 firmy Trend Micro „Wirtualni przestępcy używają obecnie klonowania głosu, jackingu SIM, modeli ChatGPT w celu analizowania sieci społecznościowych i identyfikowania podatności potencjalnych ofiar (SNAP). ChatGPT i inne narzędzia AI pomagają tworzyć systemy automatycznego gromadzenia informacji w celu identyfikacji grup docelowych ataków. Wychwytują wrażliwe zachowania, profilują je według oczekiwanej przez przestępców skali zysków, aby zaatakować ofiary (znane również jako „grube ryby”) w atakach *harpoon whaling*, *romance scams* lub nakłaniają ich do fałszywych inwestycji w kryptowaluty (*pig butchering*). Systemy LLM (Large Language Models) są również wykorzystywane do generowania złośliwego kodu wykorzystywanego w atakach cybernetycznych”.

Interesariuszy systemów cyberbezpieczeństwa można podzielić na trzy grupy. Należą do nich: struktury państwowe, przedsiębiorstwa i organizacje społeczne oraz obywatelki i obywatele.

Najważniejsze powody konieczności zapewniania państwu ochrony przed zagrożeniami cybernetycznymi:

Ochrona narodowej infrastruktury krytycznej. Wiele kluczowych sektorów, takich jak energetyka, transport, zdrowie czy finanse, opiera się na systemach informatycznych. Ataki na nie mogą prowadzić do bardzo poważnych zakłóceń w funkcjonowaniu państwa i społeczeństwa.

Obrona przed cyberwojną. W obecnych czasach wrogie państwa mogą prowadzić ataki cybernetyczne na inne państwa w celach politycznych lub militarnych. Skuteczna obrona przed takimi działaniami jest kluczowa dla utrzymania bezpieczeństwa i suwerenności państwa oraz niezakłóconego funkcjonowania instytucji państwowych i procedur demokratycznych.

Ochrona informacji rządowych. Każde państwo przechowuje wiele wrażliwych informacji, od danych osobo-

1) Wniosek w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020; Komisja Europejska, wrzesień 2022.

wych obywateli po tajne dokumenty. Ich niedostateczne zabezpieczenie może prowadzić do kradzieży tożsamości, wykorzystania wrażliwych informacji przeciwko firmom, organizacjom i obywatelom, szantażu lub innych zagrożeń.

Wśród najważniejszych powodów konieczności zapewnienia cyberbezpieczeństwa firmom są:

Zapewnienie ciągłości działania. Ataki na systemy informatyczne mogą prowadzić do zakłóceń w działalności firmy. W skrajnych przypadkach atak DDoS lub ransomware może nawet sparaliżować kluczowe operacje, prowadząc do poważnych strat finansowych. Wraz z rozwojem systemów IoT i zwiększającym się usieciowieniem infrastruktury przemysłowej, rośnie zagrożenie ataków mających na celu zakłócenia działania fizycznej infrastruktury przedsiębiorstw.

Ochrona wrażliwych danych. Firmy przechowują dane klientów, pracowników oraz własne tajemnice handlowe. Wyciek tych informacji może prowadzić do utraty zaufania klientów, strat finansowych, problemów natury prawnej oraz szkód w reputacji.

Zgodność z przepisami i regulacjami. W wielu branżach istnieją przepisy dotyczące ochrony danych, jak np. RODO w Unii Europejskiej. Firmy są zobowiązane do przestrzegania tych regulacji, co ma na celu ochronę praw obywateli. Za lekceważenie np. przepisów RODO grożą dotkliwe kary finansowe.

Dla obywateli najważniejsze z kolei są:

Ochrona prywatności i tożsamości. Współczesne społeczeństwo coraz bardziej polega na technologii. Ataki na indywidualne urządzenia lub konta mogą prowadzić do kradzieży tożsamości oraz naruszenia prywatności.

Bezpieczeństwo finansowe. Cyberprzestępcy często dokonują kradzieży pieniędzy poprzez oszustwa online lub ataki na konta bankowe. Obywatele muszą chronić swoje dane finansowe, aby uniknąć strat finansowych.

Ochrona przed przestępczością online. Internet stał się przestrzenią dla różnego rodzaju przestępstw, takich jak oszustwa, stalking czy nękanie. Właściwe praktyki cyberbezpieczeństwa pomagają się przed tym bronić.

Ochrona przed dezinformacją. Masowa dezinformacja wpływa negatywnie na interakcje społeczne, polaryzuje społeczeństwo, zaburza jego funkcjonowanie, prowadząc do zmanipulowanych działań i decyzji jednostek. Dezinformacja może prowadzić do wzrostu konfliktów społecznych, spadku zaufania i erozji kapitału społecznego, szerzenia nienawiści. Może przekładać się na obniżenie zdrowia jednostek i całego społeczeństwa, co widzieliśmy w trakcie epidemii COVID-19 jako masową kampanię antyszczepionkową. Może narażać jakość debaty publicznej i wpływać na procedury demokratyczne, obniżać zaufanie do nauki i mediów.

Podsumowując, odpowiedzią na te wszystkie zagrożenia jest wzrost cyberbezpieczeństwa. W miarę jak zagrożenia cybernetyczne ewoluują, tak samo muszą rozwijać się środki obronne, które pomogą skutecznie minimalizować ryzyko i straty.

ANALIZA OBECNEJ SYTUACJI

W tej części opracowania skupimy się na rozwoju kompetencji niezbędnych do tworzenia i płynnego funkcjonowania systemów cyberbezpieczeństwa.

Dotychczasowe działania w tym obszarze były prowadzone w dwóch kierunkach:

- rozwoju specjalistycznych zasobów, narzędzi, systemów i kompetencji
- rozwoju podstawowej świadomości co do wymagań cyberbezpieczeństwa.

Takie podejście miało wiele zalet w początkowym okresie rozwoju systemów cyberbezpieczeństwa i w dużym stopniu jest obecnie kontynuowane. Do jego mocnych stron należy koncentracja na rozwoju specjalistów, narzędzi i systemów; należy również docenić wysiłki na rzecz rozwoju podstawowej świadomości szerszych grup uczestników interakcji w cyfrowym świecie.

Jednak wraz z rozwojem cyfryzacji to podejście napotyka wiele ograniczeń, które wymuszają jego korektę lub głęboką zmianę:

- Pojawia się konieczność dopasowywania rozwiązań cyberbezpieczeństwa do wymogów konkretnych branż i segmentów z racji poszerzania cyfryzacji występujących w nich procesów biznesowych. Ale specjaliści branżowi nie otrzymują wystarczającego wsparcia w rozwoju potrzebnych im kompetencji z zakresu cyberbezpieczeństwa, a zarządy części firm nie traktują tego wyzwania jako istotnego i spychają odpowiedzialność na barki działów cyberbezpieczeństwa.
- Konieczność powszechności i spójności systemów cyberbezpieczeństwa wymaga rozwoju świadomości zagrożeń i poszukiwania nowych rozwiązań, projektowania bezpiecznych procesów w firmach, państwie i społeczeństwie, tworzenia bezpiecznych produktów i usług. Staje się to również wymogiem prawnym.
- Wraz z postępem cyfryzacji większości procesów gospodarczych i społecznych zapotrzebowanie na specjalistów cyberbezpieczeństwa gwałtownie wzrosło. Wszystkie gospodarki mierzą się z ich niedoborem, bardzo wysokimi kosztami rekrutacji oraz wymogami płacowymi. Systemowa edukacja w tej dziedzinie na świecie i w Polsce nie nadąża za potrzebami.
- Dodatkowo pogarsza się jakość pracy specjalistek i specjalistów z powodu zbyt dużej liczby obowiązków, wypalenia zawodowego i niedopasowania kompetencji do wymagań.
- Konieczność włączenia wymagań cyberbezpieczeństwa w cały cykl życia produktów i usług wymaga nowego podejścia do kompetencji wszystkich kluczowych uczestników łańcucha wartości odpowiedzialnych za projektowanie, tworzenie i produkcję, sprzedaż, dostawę, integrację, utrzymanie i serwis.

Powyższe wnioski znajdują wsparcie w licznych analizach i raportach. Jak wskazują badania firmy TrendMicro z lat 2021–2022 **62 proc. zarządzających przedsiębiorstwami widzi zapewnianie cyberbezpieczeństwa jako głównie lub całkowicie techniczne zagadnienie, a 90 proc. zgodziłoby się obejść wymagania cyberbezpieczeństwa dla realizacji innych celów biznesowych**.

Badania firmy Gartner Drivers of Secure Behavior Survey z 2022 r. wskazują, że 63–69 proc. pracowników świadomie łamiących wewnętrzne procedury, podejmuje ryzykowne działania związane z zarządzaniem hasłami, otwieraniem niezweryfikowanych linków i dokumentów, używaniem niezabezpieczonych i nieautoryzowanych urządzeń.

W sektorze publicznym mamy prawo spodziewać się podobnej percepcji, czego przykładem jest wyciek informacji z otoczenia premiera rządu, a sami obywatele mają ograniczone możliwości samodzielnego zapewniania sobie cyberbezpieczeństwa.

Szacunki przeprowadzone w 2020 r. przez Joint Research Center Komisji Europejskiej wskazywały na niedobór 1 mln specjalistek i specjalistów cyber w krajach EU i prognozowały, że na świecie w 2021 r. będzie na tych stanowiskach 3,5 mln wakatów[2].

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – w *raporcie Identifying Emerging Cyber Security Threats and Challenges for 2030*[3] wskazuje brak specjalistów i związane z tym braki kompetencyjne jako jedno z najważniejszych długoterminowych zagrożeń dla cyberbezpieczeństwa w Unii Europejskiej.

Serwis National Defence Online wskazał w czerwcu 2023 r., że w Stanach Zjednoczonych dostępnych jest prawie 700 tys. ofert pracy w dziedzinie cyberbezpieczeństwa. Z czego wynika, że „Stany Zjednoczone nie mają wystarczającej liczby specjalistów cyberbezpieczeństwa, aby chronić krajową infrastrukturę krytyczną i sieci federalne przed zagrożeniami cybernetycznymi"[4].

Według danych firmy HRK w Polsce, w 2021 r. nieobsadzonych pozostawało 17,5 tys. stanowisk dla specjalistów cyberbezpieczeństwa, a firma prognozuje ciągły wzrost tej liczby[5].

Generalnie skala niedoborów wielokrotnie przewyższa podaż specjalistów i możliwości ich edukacji w ramach obecnych programów i instytucji edukacyjnych. Niedobory specjalistów skutkują wysokimi kosztami dla gospodarki. Serwis National Defence Online wskazuje, że rekrutacja specjalistek i specjalistów cybersecurity trwa o 21 proc. dłużej niż innych specjalistów IT i wiąże się z wysokimi kosztami[6], a w Polsce według HRK „ponad połowa specjalistek i specjalistów otrzymywała od rekruterów jedną do trzech propozycji oferty pracy w ciągu tygodnia", płace w sektorze wzrosły zaś w ciągu ostatniego roku zależnie od specjalizacji od 15 do nawet 30 proc.[7].

Sytuacja ta wpływa również negatywnie na jakość pracy specjalistów cyberbezpieczeństwa. Według raportu Enterprise Strategy Group (ESG)[8] zrealizowanego wspólnie z Information Systems Security Association (ISSA) w 2021 r. 95 proc. respondentów skarżyło się na pogorszenie sytuacji w zakresie zapewniania cyberbezpieczeństwa w firmach. Jako przyczyny wskazywali wzrost liczby obowiązków obecnego personelu (62 proc.), wypalenie zawodowe (38 proc.), zatrudnianie specjalistów z niższymi niż potrzebne kwalifikacjami (29 proc.).

Wraz z poszerzaniem i pogłębianiem się cyfryzacji następuje wzrost stopnia połączenia różnych systemów informatycznych, w skład których wchodzą już nie tylko systemy komputerowe używane przez ludzi, lecz także systemy łączące obiekty fizycznej infrastruktury. W związku z tym rośnie skala zagrożeń, ponieważ „wszystko, co jest połączone, może być zaatakowane" („everything is connected, everything can be hacked"). Wielokrotnie zwiększa to skalę zagrożeń i wymagania dla zespołów cyberbezpieczeństwa.

Jednocześnie jasne jest, że wskutek opisanych wyżej braków kadrowych nie jest możliwe zapewnienie bezpieczeństwa złożonych systemów IoT tylko w oparciu o pracę specjalistów cyberbezpieczeństwa. Dlatego zakłada się przesunięcie części zadań związanych z zapewnianiem cyberbezpieczeństwa na inne grupy pracowników i ich głębsze zaangażowanie w realizację celów związanych z tym obszarem.

CYBER RESILIENCE ACT – AKT O CYBERODPORNOŚCI

W oparciu o powyższe przesłanki Komisja Europejska przygotowała pierwszą na świecie regulację (*Cyber Resilience Act*) dotyczącą produktów zawierających elementy cyfrowe.

Celem Komisji jest, z jednej strony, rozwiązanie problemu niewystarczającego poziomu cyberbezpieczeństwa w licznych produktach, w tym braku ich wystarczających aktualizacji. Jednocześnie projekt ma pomóc konsumentom i firmom oceniać poziom cyberbezpieczeństwa produktów cyfrowych oraz konfigurować je w taki sposób, aby były bezpieczne w użytkowaniu.

W praktyce Komisja planuje wprowadzić ujednolicone przepisy dotyczące obowiązkowych wymogów w zakresie cyberbezpieczeństwa podczas wprowadzania na rynek produktów posiadających elementy cyfrowe, które są bezpośrednio lub pośrednio połączone z innym urządzeniem lub siecią. Ma to obejmować sprzęt, oprogramowanie oraz usługi dodatkowe. Ponadto wymagania dotyczące cyberbezpieczeństwa mają być respektowane na etapach planowania, projektowania, rozwoju i użytkowania produktów z komponentem cyfrowym.

W związku z tą regulacją znacznemu rozszerzeniu będzie podlegał zakres działania zespołów zapewniania cyberbezpieczeństwa. Będą one zobowiązane, aby:

- przeprowadzić ocenę ryzyka związanego z używaniem przez klientów produktów i usług cyfrowych, aby zidentyfikować wynikające z nich zagrożenia dla cyberbezpieczeństwa;
- wdrożyć odpowiednie środki bezpieczeństwa w celu zminimalizowania tych zagrożeń, ich przyczyn i konsekwencji;
- testować produkty i usługi cyfrowe pod kątem podatności na zagrożenia bezpieczeństwa;
- opracować plan reagowania na incydenty związane z bezpieczeństwem w całym cyklu życia produktów;
- edukować pracowników na temat najlepszych praktyk z zakresu cyberbezpieczeństwa w całym cyklu życia produktów z komponentem cyfrowym.

Aby działy cyberbezpieczeństwa mogły sprawnie realizować te zadania, potrzebne będzie:

- zwiększenie wiedzy na temat specyfiki branż wśród pracujących w nich specjalistki i specjalistów cyberbezpieczeństwa, aby ułatwić im współpracę z innymi specjalistami i wspólnie tworzyć bezpieczne produkty i usługi;
- pogłębienie współpracy pomiędzy menedżerami zarządzającymi procesami i organizacjami zajmującymi się cyberbezpieczeństwem a menedżerami innych obszarów przedsiębiorstwa;
- odpowiednie umocowanie i rozpoznanie wagi cyberbezpieczeństwa na poziomie zarządów firm;
- rozszerzenie świadomości, wiedzy i umiejętności budowy bezpiecznych procesów, usług i produktów przez firmy i stworzenie w nich powszechnej kultury

2) Cybersecurity Our Digital Anchor. A European Perspective. Publications Office of the European Union (2020), Cybersecurity, our digital anchor - Publications Office of the EU (europa.eu) [dostęp: 06.09.2023].
3) ENISA Foresight Cybersecurity Threats for 2030 (29 marca 2023), https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 [dostęp: 06.09.2023].
4) JUST IN: U.S. Desperately Needs Cyber Talent, Congress Says (26 czerwca 2023), Naional Defence, https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says [dostęp: 06.09.2023].
5) Na rynku brakuje specjalistów od cyberbezpieczeństwa (23 października 2022), HRK, https://hrk.pl/pl/baza-wiedzy/artykuly-eksperckie/na-rynku-brakuje-specjalistow-od-cyberbezpieczenstwa [dostęp: 06.09.2023].
6) JUST IN: U.S., ibidem.
7) Na rynku brakuje specjalistów od cyberbezpieczeństwa, ibidem.
8) The Life and Times of Cybersecurity Professionals 2020 (lipiec 2023) https://www.esg-global.com/esg-issa-research-report-2020 [dostęp: 06.09.2023].

cyberbezpieczeństwa opartej o zasady *cybersecurity-by-design* i umożliwienie *cybersecurity-by-default*.

Projekt Cyber Resilience Act (CRA) po etapie konsultacji społecznych został skierowany do Parlamentu Europejskiego, gdzie po uzyskaniu pozytywnej rekomendacji Komitetu Przemysłu, Badań i Energii został przekazany pod głosowanie całej izby. Po przyjęciu przez Parlament wróci do Komisji Europejskiej, która wyda dokumenty wykonawcze obligujące państwa członkowskie do wdrożenia regulacji w ciągu następnych dwóch lat.

CRA razem z dyrektywą NIS2 (o niej poniżej), Strategią Cyberbezpieczeństwa EU i Aktem dla Cyberbezpieczeństwa tworzą podstawy organizacji i regulacji systemu cyberbezpieczeństwa w Unii Europejskiej.

NETWORK AND INFORMATION SECURITY DIRECTIVE – NIS I NIS2 ORAZ USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

W odpowiedzi na rosnącą świadomość potrzeby spójnego podejścia do kwestii cybersecurity i efektywnej ochrony infrastruktury krytycznej w EU, Parlament Europejski w 2016 r. uchwalił pierwszą Dyrektywę w sprawie bezpieczeństwa systemów informatycznych i sieciowych (NIS). Jej celem było podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego systemów informatycznych, które są kluczowe dla funkcjonowania społeczeństwa, gospodarki i sektora publicznego w krajach członkowskich. Wcześniej każdy kraj europejski radził sobie z zagrożeniami cybernetycznymi we własnym zakresie i według samodzielnie ustalonych ram.

Dyrektywa NIS koncentrowała się na opracowaniu interoperacyjnego podejścia do wysiłków przedsiębiorstw i administracji, mających na celu rozwiązanie problemów związanych z zapewnieniem cyberbezpieczeństwa i zarządzaniem ryzykiem w tym obszarze. Dyrektywa wymagała od państw członkowskich stworzenia krajowej strategii cyberbezpieczeństwa, wyznaczenia właściwych organów krajowych oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego. Ponadto nakreśliła konkretne wymagania podmiotom należącym do dwóch kategorii: Operatorzy Usług Kluczowych (OES) i Dostawcy Usług Cyfrowych (DSP).

W pracach nad regulacją wypracowano powszechnie stosowane kryteria wskazujące, które przedsiębiorstwa należą do poszczególnych kategorii i zdefiniowano związane z tym wymagania i obowiązki.

W Polsce wymagania dyrektywy NIS włączono w Ustawę o krajowym systemie cyberbezpieczeństwa, która była pierwszym aktem prawnym w tym zakresie w Polsce. Ponieważ Dyrektywa NIS jest harmonizacją minimalną, polski ustawodawca częściowo włączył w zakres ustawy również administrację publiczną oraz sektor telekomunikacyjny. Ustawa została przyjęta 5 lipca 2018 r.[9]. Obecnie regulacja przechodzi nowelizację, jednak do września 2023 r. nie została ona przyjęta przez Sejm Rzeczpospolitej Polskiej.

Jednym z kluczowych elementów systemu cyberbezpieczeństwa w UE są Operatorzy Usług Kluczowych, którzy odpowiadają za ciągłość oferowanych usług. Ich lista nie jest tożsama z utrzymywaniem 11 systemów infrastruktury krytycznej, choć w dużej mierze zakres ich odpowiedzialności pokrywa się z definicją tych systemów.

Operatorami są podmioty (zarówno przedsiębiorcy, jak i instytucje publiczne), które:

- świadczą usługi kluczowe;
- świadczenie tych usług jest zależne od systemów informacyjnych;
- incydent w tym podmiocie miałby istotny skutek zakłócający dla świadczenia tej usługi[10].

Operatorzy Usług Kluczowych odpowiadają za usługi oferowane w sektorach: energetycznym, transportowym, bankowym i za infrastrukturę rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej. Do tej ostatniej zalicza się m.in. punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen oraz rejestrów nazw domen najwyższego poziomu.

W grupie dostawców usług cyfrowych znalazły się takie podmioty jak serwisy zakupowe, wyszukiwarki internetowe oraz dostawcy usług chmurowych. Podmioty te mają spełniać inne, bardziej ograniczone wymagania niż pierwsza grupa.

Ustawa wyznaczyła również podmioty odpowiedzialne za przyjmowanie zgłoszeń i reakcję na zgłaszane incydenty bezpieczeństwa. Są to zespoły reagowania na incydenty komputerowe:

- CSIRT NASK
- CSIRT GOV
- CSIRT MON.

Ustawa tworzy także ramy dla funkcjonowania sektorowych zespołów cyberbezpieczeństwa, co jest istotnym posunięciem wprowadzającym wertykalizację cyberbezpieczeństwa i odpowiedzią na specyficzne ryzyka występujące w konkretnych branżach i konkretnych systemach (energetyka, transport itp.).

Ustawa określa ponadto ramy współpracy z innymi podmiotami zaangażowanymi w funkcjonowanie systemu cyberbezpieczeństwa w Polsce (publicznymi, instytutami badawczymi, spółkami prawa handlowego wykonującymi zadania o charakterze użyteczności publicznej czy podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa).

Wdrożenie dyrektywy i ustawy w znacznym stopniu uporządkowało system cyberbezpieczeństwa w Polsce. Przełożyło się to również na sformułowanie jasnych oczekiwań względem standardów i norm wykorzystywanych jako referencyjne w systemach zapewniania cyberbezpieczeństwa. Pomogło też lepiej zdefiniować kompetencje specjalistów cyberbezpieczeństwa.

Obecnie kluczową kwestią jest dostosowanie tej ustawy do wymagań dyrektywy NIS2 i CER oraz Aktu o Cyberodporności. Przyniesie ona m.in. zobowiązanie do skrócenia czasu raportowania incydentów, a także wymóg utworzenia dedykowanych dla cyberbezpieczeństwa jednostek organizacyjnych oraz zatrudnienie personelu z odpowiednimi poświadczeniami bezpieczeństwa.

W styczniu 2023 r. została ogłoszona i zaczęła obowiązywać w Unii Europejskiej dyrektywa NIS2. Państwa członkowskie są zobligowane do jej włączenia we własne systemy prawne do października 2024 r. Wtedy też przestaną obowiązywać zapisy pierwszej dyrektywy NIS.

Dyrektywa NIS2 wnosi do tej tematyki kilka ważnych zmian:

- zwiększa współpracę, w tym wymianę informacji, pomiędzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo w ramach Unii Europejskiej;

9) Ustawa o krajowym systemie bezpieczeństwa (28 sierpnia 2018), NASK https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa/ [dostęp: 06.09.2023].
10) Operatorzy Usług Kluczowych (15 lipca 2019), gov.pl, https://www.gov.pl/web/cyfryzacja/operatorzy-uslug-kluczowych [dostęp: 06.09.2023].

- rozszerza zakres jej stosowania na nowe grupy i poszerza zakres zadań kilku grup już objętych regulacjami NIS;
- rozszerza wymagania w zakresie zarządzania ryzykiem;
- wprowadza możliwość nakładania kar finansowych przez właściwe krajowe organy do spraw cyberbezpieczeństwa.

Raport firmy EY The *future of cybersecurity in Europe – Challenges related to the NIS2 Directive*[11] wskazuje, że organizacje, które dotąd nie podlegały dyrektywie NIS, a obejmie je dyrektywa NIS 2, będą musiały zwiększyć swoje nakłady na organizację systemu cyberbezpieczeństwa o 22 proc. Natomiast organizacje, które już były objęte regulacją NIS, powinny zwiększyć swoje budżety cybersecurity o 12 proc.

Istotna część tych szacowanych nakładów jest powiązana z zatrudnianiem nowych i rozszerzaniem kompetencji już zatrudnionych specjalistów oraz z rozszerzaniem zakresu programów budowy świadomości cyberbezpieczeństwa w organizacjach.

RAMA NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST

National Institute of Standards and Technology jest agendą Departamentu Handlu USA i od 1972 r. zajmuje się przygotowywaniem standardów i edukacją w obszarze bezpiecznego wykorzystywania technologii cyfrowych.

Najbardziej znanym produktem NIST jest model (*framework*) cyberbezpieczeństwa, który powstał w wyniku syntezy zaleceń w zakresie organizacji procesów cyberbezpieczeństwa opracowanych na podstawie dobrych praktyk w organizacjach USA. NIST jest oparty o analizę ryzyka i ma na celu przeprowadzenie następujących procesów:

1. opisanie obecnej postawy przedsiębiorstwa w zakresie cyberbezpieczeństwa;
2. opisania stanu docelowego;
3. identyfikowania i priorytetyzowania szans doskonalenia ciągłego i powtarzalnego procesu;
4. oceny postępu na drodze dążenia do stanu docelowego;
5. umożliwienia komunikacji z wewnętrznymi i zewnętrznymi interesariuszami w kwestiach ryzyka związanego z cyberbezpieczeństwem[12].

Model składa się z Rdzenia, który identyfikuje podstawowe funkcje najważniejszych procesów związanych z organizacją systemu zapewniania cyberbezpieczeństwa. Funkcjami tymi są:

- Identyfikacja
- Ochrona
- Wykrywanie
- Reagowanie
- Przywracanie.

Źródło: National Institute of Standards and Technology

Funkcje są podzielone na Kategorie, ściśle powiązane z konkretnymi potrzebami i określonymi czynnościami procesu zapewniania cyberbezpieczeństwa. Przykłady takich kategorii to: „Zarządzanie Aktywami", „Kontrola Dostępu" czy „Procesy Detekcji".

Kategorie są podzielone na Podkategorie, będące już wąsko zdefiniowanymi definicjami oczekiwanego stanu realizacji czynności, np.: „Zewnętrzne systemy informacyjne są skatalogowane", „Dane stacjonarne są chronione" czy „Powiadomienia z systemów detekcji są kontrolowane".

Do każdej podkategorii są również przypisane Odniesienia Informacyjne, które nawiązują do konkretnych norm, wytycznych standardów i powszechnych praktyk związanych z ograniczeniem ryzyka w obszarze cyberbezpieczeństwa. Przykładowe odniesienia to normy ISO/IEC 27001 czy ISA/IEC 62443 (rodzina standardów, wytycznych oraz dobrych praktyk służących zabezpieczeniu systemów sterowania i automatyki przemysłowej).

Cała matryca składa się z 23 kategorii i 108 podkategorii opisujących całe spektrum działań w zakresie cyberbezpieczeństwa.

Kolejnym wymiarem modelu jest poziom pokazujący stopień realizacji wymagań i odnosi się do trzech obszarów:

- Procesu zarządzania ryzykiem
- Zintegrowanego programu zarządzania ryzykiem
- Współpracy z zewnętrznymi podmiotami ekosystemu

Model wskazuje 4 poziomy określające:

Częściową realizację wytycznych. W tym przypadku istnieje ograniczona świadomość zagrożeń cybernetycznych na poziomie organizacyjnym, a systemowe podejście do zarządzania zagrożeniami cybernetycznymi nie zostało opracowane.

Poziom świadomości ryzyka. W organizacji istnieje świadomość zagrożeń cybernetycznych, ale całościowe podejście do zarządzania zagrożeniami cybernetycznymi nie zostało opracowane. Procesy i procedury biorące pod uwagę ryzyko i zatwierdzone przez zarząd zostały zdefiniowane i wdrożone, personel posiada wystarczające zasoby do wykonywania swoich obowiązków związanych z cyberbezpieczeństwem. Informacje na temat cyberbezpieczeństwa są przekazywane w organizacji w postaci nieformalnej.

Osiągnięcie powtarzalnych możliwości. Tu polityka, procesy i procedury świadome ryzyka zostały zdefiniowane, wdrożone zgodnie z oczekiwaniami i skontrolowane. Wdrożone zostały spójne metody skutecznego reagowania na zmiany ryzyka. Personel ma wiedzę i umiejętności do realizacji swoich wyznaczonych ról i odpowiedzialności.

Poziom możliwości adaptacyjnych. Organizacja doskonali swoje praktyki w zakresie cyberbezpieczeństwa na podstawie doświadczeń i przewidywalnych wskaźników uzyskanych z poprzednich i obecnych czynności związanych z cyberbezpieczeństwem. W drodze ciągłego doskonalenia obejmującego zaawansowane technologie i praktyki cyberbezpieczeństwa organizacja aktywnie adaptuje się do zmieniającego się otoczenia cyberbezpieczeństwa i w odpowiednim czasie reaguje na ewoluujące i złożone zagrożenia. Zarządzanie ryzykiem związanym z cyberbezpieczeństwem stanowi część kultury organizacyjnej, a organizacja aktywnie komunikuje się i współpracuje w ramach ekosystemu cyberbezpieczeństwa.

Aby osiągnąć minimalizację ryzyka zagrożeń cybernetycznych, organizacje powinny dążyć do czwartego poziomu.

Ważnym elementem modelu są rekomendacje integracji systemu zapewniania cyberbezpieczeństwa z procesami zarządczymi w organizacji. Model kładzie duży nacisk na wagę zrozumienia przez zarządzających warunków i zasad integracji procesów cyberbezpieczeństwa z wymaganiami biznesowymi i regułami ładu korporacyjnego.

11) Future of cybersecurity in Europe – Challenges related to the NIS2 Directive (2023), EY, https://assets.ey.com/content/dam/ey-sites/ey-com/pl_pl/noindex/2023/ey-raport-nis2.pdf [dostęp: 06.09.2023].
12) Ramy Usprawniania Cyberbezpieczeństwa Krytycznej Infrastruktury, www.nist.gov, 2014

Wieloletnia praktyka stosowania modelu doprowadziła do identyfikacji potrzeby zindywidualizowania podejścia i dopasowania go do wymogów wybranych branż, segmentów i grup zastosowań. Obecnie przygotowane są następujące profile:

- Cybersecurity Framework Manufacturing Profile
- Cybersecurity Framework Smart Grid Profile
- Cybersecurity Framework Profile Excel for Connected Vehicle Environments
- Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure
- Maritime Cybersecurity Framework Profiles
- Cybersecurity Framework Profile for Communications Sector
- Cybersecurity Framework Profile for Hybrid Satellite Networks
- Cybersecurity Framework Profile for Liquefied Natural Gas
- Cybersecurity Framework Election Infrastructure Profile
- Cybersecurity Framework Botnet Threat Mitigation Profile – Cybersecurity Coalition
- Cybersecurity Framework DDoS Threat Mitigation Profile

Liczba i zróżnicowanie tych profili podkreślają rolę głębokiej integracji funkcji cyberbezpieczeństwa z wymaganiami biznesowymi poszczególnych branż i konieczność specjalizacji cyberbezpieczeństwa ze względu na specyfiki infrastruktury technicznej i softwarowej oraz procesów i wykorzystywanych w danej branży narzędzi cyfrowych. Odzwierciedla to również fakt powszechnej integracji infrastruktury fizycznej z sieciami komputerowymi.

Obecnie trwa proces aktualizacji NIST, który zostanie zakończony w 2024 r. W sierpniu 2023 r. zostały zarysowane pierwsze istotne zmiany w strukturze modelu. Najważniejszą z nich jest podkreślenie wagi kwestii organizacyjnych i zarządczych poprzez dodanie nowej funkcji do dotychczasowych pięciu. Jest nią „Govern" – Zarządzanie. Warto zwrócić uwagę na jej horyzontalny zakres, bo to podstawa realizacji wszystkich pozostałych. Wprowadzenie tak istotnej zmiany jest motywowane następująco:

„Do tej pory model Cybersecurity Framework opisywał filary programu cyberbezpieczeństwa, wykorzystując pięć głównych funkcji: identyfikację, ochronę, wykrywanie, reagowanie i odbudowę. Do nich NIST dodał teraz szóstą funkcję – zarządzanie, która obejmuje sposób, w jaki organizacja może podejmować i wdrażać własne decyzje w celu realizacji strategii cyberbezpieczeństwa. Ten ruch podkreśla, że cyberbezpieczeństwo jest głównym źródłem ryzyka dla przedsiębiorstwa, obok ryzyka prawnego i finansowego, które są podstawowymi obszarami ryzyka, branymi pod uwagę przez kierownictwo"[13].

Proponowana nowa struktura matrycy wygląda jak poniżej:

Źródło: NIST Drafts Major Update to Its Widely Used Cybersecurity Framework

13) NIST Drafts Major Update to Its Widely Used Cybersecurity Framework (8 sierpnia 2023), NIST, https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework [dostęp: 06.09.2023].

Model NIST jest najpopularniejszym na świecie standardem i materiałem referencyjnym. Został pobrany ponad 2 mln razy przez użytkowników z 185 krajów, a przetłumaczono go na dziewięć języków. Model jest ciągle aktualizowany i rozwijany, co daje gwarancję jego wartości i użyteczności.

ISO/EIC 27001 – WYMAGANIA DLA SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

W Europie kontynentalnej jednym z najbardziej rozpoznawalnych i popularnych standardów dla organizacji systemów zarządzania ryzykiem i zapewniania cyberbezpieczeństwa jest międzynarodowy standard ISO/IEC 27001[14]. Początkowo kładł on duży nacisk na kwestie bezpieczeństwa informacji, ale w wyniku kolejnych zmian został rozszerzony do postaci obejmującej swym zakresem systemowe zapewnianie bezpieczeństwa i ciągłości operacji biznesowych, szeroko rozumianego bezpieczeństwa informacji oraz zapewniania prywatności.

Standard ten został opracowany przez International Organization for Standardization (ISO) oraz International Electrotechnical Commission (IEC). Obecnie jest wykorzystywana jego trzecia wersja, opublikowana w październiku 2022 r. i określona symbolem ISO/IEC 27001:2022. Zastąpiła ona normę ISO/IEC 27001:2013, opublikowaną prawie 10 lat wcześniej i później dwukrotnie aktualizowaną. Pierwsze rekomendacje dla ochrony bezpieczeństwa informacji zostały opublikowane w 2005 r.

Najnowsza wersja normy ma liczne uzupełnienia i dotyka większego obszaru aktywności różnych organizacji niż tylko wąsko pojmowane cyberbezpieczeństwo:

- skupia się na korzyściach biznesowych;
- podchodzi całościowo do aktywności organizacji;
- wzmacnia odporność funkcjonowania organizacji;
- bierze pod uwagę cały łańcuch dostaw i łańcuch wartości;
- obejmuje całe spektrum zarządzania informacją, bez względu na jej formę zapisu;
- uwzględnia zarówno systemy informatyczne, jak i infrastrukturę fizyczną oraz wszystkich ludzi funkcjonujących w firmie;
- pomaga w spełnieniu wymagań regulacyjnych i prawnych;
- porządkuje całościowo procesy przepływu informacji w przedsiębiorstwie;
- pomaga w uporządkowaniu procesów biznesowych.

Standard jest oparty o ocenę ryzyka i zarządzanie ryzykiem. ISO27001 to konstrukcja wielowymiarowa. Definiuje kluczowe odpowiedzialności i zadania, które powinny umożliwiać prawidłowe przygotowanie, wdrożenie i utrzymanie systemu zarządzania informacją i bezpieczeństwem. W kolejnym wymiarze definiuje konkretne obszary, które dla realizacji wszystkich funkcji systemu powinny podlegać kontroli, ocenie ryzyka i zarządzaniu.

Z perspektywy organizacji procesu zarządzania bezpieczeństwem informacji standard wyróżnia następujące elementy:

1. Budowa środowiska bezpieczeństwa w organizacji opartego na jej dogłębnym zrozumieniu
   - w tym głównych procesów, zaangażowanych w nie stron i korzyści, jakie są dla nich kluczowe z perspektywy systemu zarządzania bezpieczeństwem informacji;
   - i określeniu zakresu działania tego systemu.

14) ISO/IEC 27001 — Information security management systems: https://www.iso.org/standard/27001.

2. Przygotowanie wsparcia liderów organizacji dla funkcjonowania takiego systemu

- zdefiniowanie celów i korzyści dla całej organizacji i ich artykulacja;
- integracja wymagań systemu zarządzania bezpieczeństwem informacji i organizacji procesów biznesowych funkcjonujących w firmie;
- zapewnienie zasobów potrzebnych do budowy systemu, jego utrzymania i rozwoju;
- pokazywanie bieżących korzyści z funkcjonowania systemu i istotności stosowania jego reguł i wymagań;
- wspieranie rozwoju nowych funkcji systemu odnoszących się do nowych procesów i nowych obszarów ryzyka;
- zapisanie celów i zasad funkcjonowania systemu w formie jasnych wymagań i procedur;
- komunikacja procedur, wymagań i polityki zarządzania bezpieczeństwem informacji;
- przypisanie jasnej odpowiedzialności oraz formalnych uprawnień organizacyjnych w celu wsparcia sprawności systemu i realizacji jego celów;
- regularne przygotowywanie oraz regularne prezentowanie informacji o funkcjonowaniu systemu na forum zarządzających daną organizacją.

3. Stworzenie planu funkcjonowania systemu

- określenia źródeł ryzyka, kryteriów jego oceny oraz poziomów akceptacji i przypisania do nich odpowiednich działań;
- określenia właścicieli procesów, których dotyczą ryzyka;
- określenie ryzyka z punktu widzenia zarządzania informacją oraz poufności, integralności i dostępności informacji;
- określenia potencjalnych konsekwencji związanych z realizacją ryzyka w poszczególnych obszarach;
- określenia priorytetów z perspektywy zarządzania ryzykiem w poszczególnych obszarach;
- określanie działań związanych z obniżaniem poziomu ryzyka dla poszczególnych obszarów i konkretnych elementów procesów;
- zapisania planu i uzyskanie akceptacji dla jego wdrożenia i realizacji;
- przygotowania mierników realizacji planu;
- przygotowania mierników oceny funkcjonowania systemu zarządzania bezpieczeństwem informacji w organizacji;
- określenie sposobu komunikacji stopni ryzyka i poziomu działania systemu w poszczególnych obszarach;
- zdefiniowanie sposobu reakcji i dostosowania organizacji do oceny ryzyka i sposobów funkcjonowania systemu zarządzania bezpieczeństwem informacji.

4. Przygotowanie zasobów potrzebnych dla systemu zarządzania bezpieczeństwem informacji z uwzględnieniem:

- zasobów czasu i środków dla pokrycia kosztów przygotowania i działania systemu;
- kompetencji potrzebnych w organizacji do przygotowania, wdrożenia i utrzymania funkcjonowania takiego systemu;
- oceny wyjściowego stanu kompetencji;
- oceny planu rozwoju i aktualizacji kompetencji poprzez system szkoleń, dostarczania wiedzy i oceny sprawności współpracy;
- udokumentowania wymagań kompetencyjnych w obszarze zapewniania bezpieczeństwa informacji;
- uzyskiwania wymaganego poziomu świadomości odnośnie systemu i jego wymagań;
- określenia zasobów potrzebnych do dokumentacji pracy systemu i komunikacji o jego wymaganiach i pracy;

5. Przygotowanie zasad zarządzania informacją

- zdefiniowanie, co ma być zapisywane;
- w jakiej formie;
- na jakich nośnikach;
- określenia formy zapisu, autora, sposobów aktualizacji;
- przypisanie poziomów poufności;
- zasady dostępu do informacji na poszczególnych poziomach;
- sposoby przechowywania informacji;
- kontrola wersji;
- zasady usuwania informacji.

6. Wsparcie funkcjonowania systemu poprzez:
   - ustalenie częstotliwości oceny ryzyka i zasad tego procesu;
   - określenie sytuacji, które wymagają korekty lub rozszerzenia zasad oceny ryzyka;
   - zdefiniowanie i realizację funkcji monitorowania, mierzenia, analizy i oceny ryzyka i działań związanych z zarządzaniem ryzykiem.
7. Wykonywanie audytów
   - określanie zasad audytu sposobu funkcjonowania systemu zarządzania bezpieczeństwem informacji;
   - realizacja audytów.
8. Dokonywanie przeglądów zarządczych
9. Planowanie i przygotowywanie rozwoju systemu

Jest to bardzo szczegółowy i precyzyjny opis systemu z perspektywy jego organizacji i wsparcia. Jest on szeroko rozpisany i przypisuje odpowiedzialność za jego funkcjonowanie na każdym poziomie zarządzania, ze szczególnym uwzględnieniem odpowiedzialności menedżerów różnego szczebla. To podejście zakłada również bardzo wysoki poziom zaangażowania zarządu i wyższego szczebla zarządzających w funkcjonowanie systemu zarządzania bezpieczeństwem informacji.

Dokumentacja standardu podkreśla konieczność realizacji wszystkich tych wymagań łącznie i akcentuje ich współzależność.

Standard ISO27001 z praktycznej perspektywy oceny i minimalizacji ryzyka skupia się na następujących kwestiach:

- zarządzanie systemem zapewniania bezpieczeństwa
- zarządzanie ryzykiem
- zgodność prawna i regulacyjna
- bezpieczeństwo w polityce zasobów ludzkich
- bezpieczeństwo w łańcuchu wartości i dostaw
- kontrola bezpieczeństwa i dostępu
- zarządzanie środkami trwałymi
- bezpieczeństwo informacji
- bezpieczeństwo systemów, sieci i aplikacji
- zarządzanie podatnością i zagrożeniami
- zarządzanie incydentami

Są one w ramach standardu ISO27001 podzielone na następujące obszary:

1. organizacja firmy i systemu zarządzania informacją;
2. zasady zatrudnienia personelu i zasady funkcjonowania pracowników i innych osób w organizacji;
3. zapewnianie kontroli fizycznego dostępu, funkcjonowania fizycznej infrastruktury i wykorzystywania urządzeń;
4. zapewniania cyberbezpieczeństwa i informatycznych aspektów funkcjonowania infrastruktury cyfrowej.

W ramach poszczególnych obszarów ocenie i kontroli podlegają konkretne aspekty działalności firmy i konkretne procesy. I tak:

W obszarze organizacja badanych jest 37 procesów, m.in.: procedury bezpieczeństwa informacji, podział ról i odpowiedzialności dla zapewniania działania systemu zarządzania bezpieczeństwem informacji, podział odpowiedzialności, przypisanie odpowiedzialności do zarządu, kontakt z organami regulacyjnymi i organami ścigania, ale i zasady poufności, zasady kontroli dostępu, zasady zarządzania informacją w łańcuchu dostaw i wartości, wymagania prawne, ustawowe, regulacyjne i umowne organizacji, gotowość systemów ICT dla wsparcia ciągłości działania operacji biznesowych oraz zasady wykorzystywania sprzętu przypisanego do pracowników.

W obszarze zasad zatrudniania personelu i zasad funkcjonowania personelu w organizacji ujętych jest osiem procesów, w tym: screening, zasady zawierania i rozwiązywanie umów o pracę, zasady szkoleń z obszaru zarządzania informacją, zasady zarządzania informacją w procesach dyscyplinarnych, zasady utrzymywania poufności informacji (NDA) oraz zasady bezpieczeństwa informacji w warunkach pracy zdalnej.

W obszarze zapewnianie kontroli fizycznego dostępu, funkcjonowania fizycznej infrastruktury i wykorzystywania urządzeń ujętych jest 14 elementów, w tym takie jak: zasady kontroli fizycznego dostępu, zasady monitorowania pomieszczeń i obszaru firmy, zabezpieczanie pomieszczeń i budynków, ale też polityka clear desk & clear screen, zarządzanie całym cyklem życia fizycznych nośników informacji, zabezpieczenia przed skutkami klęsk żywiołowych, zapewnianie dostępu do mediów w sytuacjach kryzysowych, zasady wykorzystywania, wprowadzania do użytku i wycofywania sprzętu.

Trzy powyższe obszary są ściśle powiązane z kwestiami cyberbezpieczeństwa, jednak traktują zarządzanie bezpieczeństwem informacji znacznie szerzej. Obszary te odnoszą się w dużej mierze do funkcji Identify i Protect w matrycy NIST.

Z kolei czwarty obszar odnosi się bezpośrednio do cyberbezpieczeństwa.

W obszarze zapewniania cyberbezpieczeństwa i informatycznych aspektów funkcjonowania infrastruktury cyfrowej zawarte są 33 punkty i procesy kontroli. Są to:

LP	OBSZAR KONTROLI LUB PROCES
1	Urządzenia końcowe
2	Definicja praw dostępu
3	Ograniczenia dostępu do informacji
4	Dostęp do kodów źródłowych
5	Uwierzytelnianie
6	Zarządzanie dostępnością zasobów
7	Ochrona przed złośliwym oprogramowaniem
8	Zarządzanie podatnością
9	Zarządzanie konfiguracją
10	Usuwanie danych i informacji
11	Maskowanie danych
12	Zapobieganie wyciekom danych

13	Tworzenie kopii zapasowych
14	Redundancja kluczowych procesów
15	Zapisywanie stanów systemów (logów)
16	Monitorowanie zdarzeń w sieciach, systemach i aplikacjach
17	Synchronizacja czasu
18	Wykorzystanie oprogramowania o uprzywilejowanych prawach dostępu
19	Instalacja oprogramowania w instancjach i systemach biznesowych (produkcyjnych)
20	Bezpieczeństwo sieci
21	Bezpieczeństwo usług sieciowych
22	Segregacja sieci
23	Filtrowanie treści
24	Wykorzystanie kryptografii
25	Zabezpieczanie cyklu życia produktu
26	Stosowanie wymagań bezpieczeństwa
27	Bezpieczna architektura systemów
28	Tworzenie bezpiecznego kodu
29	Bezpieczne testy i rozwój oprogramowania
30	Kontraktowanie zewnętrznego rozwoju oprogramowania
31	Separacja środowisk rozwoju, testowania i wykorzystania oprogramowania
32	Zarządzanie wersjami i zmianami w oprogramowaniu
33	Zapisywanie informacji z testów
34	Ochrona informacji i systemów w trakcie procedur audytowych

Źródło: ISO/EIC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements http://www.itref.ir/uploads/editor/2ef522.pdf.

Obszar opisany jest spójny z większością funkcji w matrycy NIST. W sposób bezpośredni do funkcji *Protect* i *Detect*, a poprzez spojrzenie z perspektywy procesowej pozwala na odniesienia do funkcji *Respond* i *Recover*.

Standard ISO27001 jest skorelowany i odnosi się do innych standardów, narzędzi i realizowanych przez nie koncepcji cyberbezpieczeństwa:

- Z perspektywy zarządzania informacja odnosi się do triady: CIA – poufność, integralność i dostępność informacji.
- Odnosi się również do typów działań w obszarze cybersecurity: *Protect, Detect, Correct*.

Zapewnia to dużą spójność podejścia i w całościowy sposób obejmuje operacyjne działania dla zapewnienia ciągłości biznesowej i odporności na zakłócenia, z uwzględnieniem bezpieczeństwa informacji, bezpieczeństwa infrastruktury fizycznej i cyberbezpieczeństwa. W sumie wdrożenie w organizacji standardu ISO 27001 tworzy bardzo solidny fundament dbania o jej cyberbezpieczeństwo.

W Polsce norma PN-EN ISO/IEC 27001 jest wykorzystywana m.in. przez Operatorów Usług Kluczowych do określania wymagań wobec systemów zarządzania bezpieczeństwem informacji.

UK INITIAL NATIONAL CYBER SECURITY SKILLS STRATEGY

Rada UK Cyber Security Council została powołana przez odpowiedzialny za cyberbezpieczeństwo w Zjednoczonym Królestwie Department for Digital, Culture, Media and Sport. Stało się to we wrześniu 2019 r. Rada jest rozwinięciem działań konsorcjum Cyber Security Alliance, zrzeszającego różne organizacje zainteresowane rozwojem cyberbezpieczeństwa w Wielkiej Brytanii.

Rada zajmuje się wsparciem realizacji strategii rozwoju kompetencji dla cyberbezpieczeństwa Initial National Cyber Security Skills Strategy[15], opublikowanej w grudniu 2018 r.

Strategia jest bardzo wartościowym dokumentem, ponieważ precyzyjnie patrzy na rozwój i zapewnianie cyberbezpieczeństwa z perspektywy rozwoju kompetencji. Kompetencje dla cyberbezpieczeństwa definiuje jako:

„(...) połączenie podstawowej i zaawansowanej wiedzy oraz umiejętności technicznych, umiejętności strategicznego zarządzania, umiejętności planowania i organizacji oraz uzupełniających umiejętności miękkich, które pozwalają organizacjom na:

- zrozumienie bieżących i potencjalnych przyszłych zagrożeń cybernetycznych, z jakimi się one mierzą
- tworzenie i poszerzanie świadomości zagrożeń cybernetycznych, dobrych praktyk oraz zasad lub koniecznych do przestrzegania polityk, zarówno na wyższych jak i niższych szczeblach organizacji
- wdrażanie technicznego systemu kontroli i wykonywanie zadań niezbędnych do ochrony organizacji, opartych na dokładnym zrozumieniu poziomu zagrożenia
- spełnianie wymagań formalnych i prawnych w zakresie cyberbezpieczeństwa, takich jak obowiązki prawne dotyczące ochrony danych
- skuteczne prowadzenie analiz i inspekcji oraz reagowanie na bieżące i potencjalne przyszłe ataki cybernetyczne”[16].

Funkcje, które mają realizować osoby z kompetencjami cyberbezpieczeństwa, są generalnie spójne z modelem NIST i innymi dokumentami. Na uwagę zasługuje jednak wyraźne podkreślanie, że w zapewnianiu cyberbezpieczeństwa obok umiejętności technicznych konieczne są umiejętności organizacyjne (zarządzania strategicznego, planowania i organizacji) oraz kompetencje miękkie, umożliwiające skuteczną pracę specjalistów w zespołach organizacji. Słowem – wszystkie trzy grupy kompetencji są istotne dla prawidłowej realizacji zadań dotyczących cyberbezpieczeństwa.

Brytyjska strategia cechuje się jeszcze dwoma interesującymi elementami. Kładzie nacisk na promocję edukacji specjalistów cyberbezpieczeństwa o różnych profilach wykształcenia, specjalistów innych branż, z innym wykształceniem niż techniczne.

Drugim elementem jest integracja wymagań cyberbezpieczeństwa z procesami biznesowymi, co przekłada się na trzy grupy działań:

15) Initial National Cyber Security Skills Strategy, HM Government https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/949211/Cyber_security_skills_strategy_211218_V2.pdf [dostęp: 06.09.2023].

16) Ibidem, str. 20.

- szerokie podstawowe szkolenia z zakresu cyberbezpieczeństwa dla ogółu pracowników;
- włączanie wymagań cyberbezpieczeństwa do profili kompetencji osób zarządzających organizacjami na różnych szczeblach i w organizacjach o różnej wielkości i charakterze;
- włączania wymogów cyberbezpieczeństwa w reguły funkcjonowania wielu innych branż, m.in. budownictwa, finansów, służby zdrowia, transportu czy przemysłu.

CYBER SECURITY BODY OF KNOWLEDGE

Kolejnym istotnym elementem strategii cyberbezpieczeństwa w Wielkiej Brytanii jest Cyber Security Body of Knowledge[17], który to organ funkcjonuje zarówno niezależnie, jak i mieści się w strukturach brytyjskiego National Cyber Security Center.

Celem powołania tego organu było skodyfikowanie i uporządkowanie wiedzy z zakresu cyberbezpieczeństwa, aby pomóc w budowaniu programów edukacyjnych adresowanych do specjalistów w tym obszarze. Wysiłek ten został podjęty z powodu dużego rozproszenia wiedzy, szybkiego tempa jej przyrostu i ogólnie niskiej dojrzałości całego ekosystemu. W ciągu prawie trzech lat, 115 specjalistek specjalistów z całego świata pracowało nad opracowaniem pierwszej wersji dokumentu, który został opublikowany w 2019 r., a w lipcu 2021 r. opublikowano jego uaktualnioną wersję CyBOK version 1.1.

W dokumencie uporządkowano zebraną wiedzę w 21 obszarach (*Knowledge Areas*), podzielonych na pięć szerszych grup:

1. **Human, Organisational and Regulatory Aspects** (Aspekty ludzkie, organizacyjne i regulacyjne)
2. **Attacks and Defences** – Ataki i obrona
3. **Systems Security** – Bezpieczeństwo systemów
4. **Software and Platform Security** – Bezpieczeństwo oprogramowania i platform
5. **Infrastructure Security** – Bezpieczeństwo infrastruktury

CyBOK zawiera podstawowe definicje, odnosi się do najbardziej znanych narzędzi, jak rama NIST, uwzględnia perspektywę *cybersecurity-by-design* i *cybersecurity-by-default* i zbiera olbrzymi zasób wiedzy w każdym obszarze. Cały dokument ma ponad 1000 stron i stanowi jedno z najpopularniejszych źródeł wiedzy i punkt odniesienia w niemal każdej dyskusji o cyberbezpieczeństwie.

W sumie brytyjska strategia prezentuje najbardziej pełne i szeroko zakrojone podejście do cyberbezpieczeństwa, bardzo dobrze skoordynowane z systemem całej gospodarki, edukacji i różnymi aspektami funkcjonowania społeczeństwa.

SZEROKIE PODEJŚCIE DO CYBERBEZPIECZEŃSTWA W WIELKIEJ BRYTANII

Wraz z postępującą wertykalizacją i specjalizacją oraz wzrostem zakresu odpowiedzialności specjalistów cyberbezpieczeństwa za produkty i usługi w całym cyklu ich życia, rośnie rola współpracy i integracji funkcji cyberbezpieczeństwa z funkcjami operacyjnymi i zarządczymi w przedsiębiorstwach, organizacjach i administracji.

Ta ewolucja wymaga przystosowania i przygotowania procesów cyberbezpieczeństwa do rozszerzenia zakresu przedmiotowego oraz dobrego przygotowania specjalistów z obu grup: cyberbezpieczeństwa i operacji biznesowych. Wielka Brytania jest dobrym przykładem, jak to robić.

Już na początku drugiej dekady XXI w. sformułowano wizję stanowiącą podstawę późniejszego rozwoju strategii cyberbezpieczeństwa, która mówiła, że Wielka Brytania ma być najbezpieczniejszym miejscem do pracy i życia w sferze online[18]. Było to w tamtym czasie szersze spojrzenie niż w większości innych krajów, które ograniczały swoją perspektywę do ochrony infrastruktury i systemów.

To podejście zaowocowało silną artykulacją priorytetów współpracy pomiędzy obszarami biznesu, nauki i branży cybersecurity oraz wzmocnieniem roli współpracy pomiędzy funkcjami operacyjnymi, zarządczymi oraz technicznymi w organizacji.

Utworzone w Wielkiej Brytanii w 2016 r., The National Cyber Security Centre[19] od początku swojego działania kładzie duży nacisk na komunikację z szerokimi grupami odbiorców usług zapewniania cyberbezpieczeństwa. Już w 2017 r. zostały przygotowane zalecenia dla małych i średnich przedsiębiorstw, a w marcu 2018 r. NCSC rozpoczęło szerokie kampanie informacyjne dotyczące dbałości o cyberbezpieczeństwo.

W 2020 r. zostały przygotowane pierwsze standardy i założenia implementacji praktyk związanych z podejściem *cybersecurity by design*. Finalnie powstały zalecenia odnośnie do edukacji różnych grup w ramach ekosystemu cyberbezpieczeństwa, wraz z określeniem odpowiedzialności i zasad ich współpracy.

NCSC przygotowało zalecenia dla:

- obywatelek, obywateli i rodzin
- osób prowadzących jednoosobowe działalności gospodarcze
- małych i średnich firm – SMB
- dużych organizacji
- sektora publicznego
- technicznych specjalistów cyberbezpieczeństwa.

W materiałach przygotowanych dla firm bardzo dużo uwagi poświęca się kwestiom przypisania odpowiedzialności za realizację funkcji cyberbezpieczeństwa zarządom organizacji oraz kwestiom włączenia wymogów cyberbezpieczeństwa do wszystkich obszarów ich działania. Jako kluczowe zasady współpracy działów cybersecurity z resztą organizacji uznano:

- wdrożenie wymogów cyberbezpieczeństwa w całej organizacji
- identyfikacja krytycznych zasobów w organizacji
- rozwijanie pozytywnej kultury bezpieczeństwa cybernetycznego
- nieustanny rozwój wiedzy w tym zakresie
- budowa świadomości zagrożeń dla bezpieczeństwa cybernetycznego
- zarządzanie ryzykiem w zakresie cyberbezpieczeństwa
- wdrażanie skutecznych środków bezpieczeństwa cybernetycznego
- współpraca z łańcuchem dostaw i partnerami
- planowanie reakcji na incydenty cybernetyczne[20].

Wszystkie te zagadnienia zostały uszczegółowione i rozpisane na konkretne pytania sprawdzające stopień przygotowania organizacji w poszczególnych obszarach. Sam materiał dla zarządzających można znaleźć w opublikowanym w marcu 2023 r. materiale Cyber Security Toolkit for Boards, który jest umieszczony w witrynie NCSC pod adresem https://www.ncsc.gov.uk/collection/board-toolkit.

17) The Cyber Security Body Of Knowledge: https://www.cybok.org/.

18) Policy paper 5. A safe and secure cyberspace - making the UK the safest place in the world to live and work online (1 marca 2017), gov.uk, https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe--and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online [dostęp: 06.09.2023].

19) The National Cyber Security Centre – https://www.ncsc.gov.uk/.

20) Cyber Security Toolkit for Boards, NCSC, https://www.ncsc.gov.uk/collection/board-toolkit/toolkits-toolbox/briefing-packs [dostęp: 06.09.2023].

Konsekwentna realizacja podejścia zorientowanego na bliską współpracę pomiędzy specjalistami cyberbezpieczeństwa i zarządzającymi w celu włączenia wymagań *cyber* we wszystkie procesy firmy przyniosła oczekiwane efekty. Według Cyber Security Breaches Survey[21] z lipca 2022 r., czterech na pięciu (82 proc.) członków zarządów lub kadry kierowniczej wyższego szczebla w brytyjskich firmach, ocenia priorytet bezpieczeństwa cybernetycznego jako „bardzo wysoki" lub „dość wysoki".

Dodatkowo 80 proc. zarządów otrzymuje informacje o stanie bezpieczeństwa cybernetycznego firmy co najmniej raz na kwartał, 63 proc. firm przeprowadziło ocenę ryzyka, a 61 proc. przeprowadziło szkolenie personelu. W przypadku mniejszych firm te dane kształtują się na poziomie odpowiednio 50 proc., 33 proc. i 17 proc.

W Polsce, w 2021 r. Państwowy Instytut Badawczy NASK, odpowiedzialny również za prowadzenie jednego z trzech państwowych CERTów i edukację w zakresie cyberbezpieczeństwa, przeprowadził badanie E-transformacja i bezpieczeństwo cyfrowe w polskich przedsiębiorstwach[22]. Wzięło w nim udział 120 firm i z końcowego raportu wynika, że:

„Na pytanie o to, czy w ostatnim czasie w firmie odnotowano naruszenia bezpieczeństwa cyfrowego, większość przedstawicieli MŚP odpowiedziała, że nie (64,2 proc.). Badani nie wymienili takich zagrożeń jak phishing czy spam) (...) Te odpowiedzi obrazują rzeczywisty stan infrastruktury IT w najmniejszych firmach, gdzie jest ona zawężona najczęściej do podstawowych narzędzi systemowych. Umiejętność identyfikacji takich zdarzeń jest powiązana z kompetencjami użytkowników. W firmie, gdzie jedna osoba odpowiada za całą firmę i, nie ma działu IT, cyberataki mogą być nierozpoznane, jeśli tylko nie zablokują działania podstawowych narzędzi takich jak skrzynka e-mail itp.".

I dalej:

„Mając na uwadze odpowiedzi na temat planów i inwestycji w cyberbezpieczeństwo, wskazujące na znikome zainteresowanie takimi rozwiązaniami, można wnioskować, że właściciele lekceważą zagrożenia i nie widzą barier, bo uważają, że cyberzagrożenia nie dotyczą ich firmy. Brak rozbudowanych systemów usprawniających czy też sama wielkość przedsiębiorstwa, zdaniem respondentów wyklucza takie ryzyko".

Analiza zasobów udostępnionych w witrynie www.nask.pl pokazuje, że można tam znaleźć informacje o państwowym systemie cyberbezpieczeństwa oraz o działaniach i narzędziach wykorzystywanych i stworzonych przez NASK, jednak nie ma tam zasobów dedykowanych bezpośrednio firmom, organizacjom i obywatelom.

Materiały w języku polskim ze wskazówkami dotyczącymi organizacji procesów cyberbezpieczeństwa w małych i średnich firmach można za to znaleźć na stronach ENISA – Agencji Unii Europejskiej ds. Cyberbezpieczeństwa. W 2021 r. opublikowała ona Przewodnik po bezpieczeństwie cybernetycznym dla MŚP – 12 kroków do bezpieczeństwa twojej firmy[23].

21) Official Statistics. Cyber Security Breaches Survey 2022 (11 lipca 2022), gov.uk, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 [dostęp: 06.09.2023].
22) E-transformacja i bezpieczeństwo cyfrowe w polskich przedsiębiorstwach (22.04.2021), NASK, https://www.nask.pl/pl/raporty/raporty/4178,E-transformacja-i-bezpieczenstwo-cyfrowe-w-polskich-przedsiebiorstwach-pilotaz.html [dostęp: 06.09.2023].
23) 12 kroków do bezpieczeństwa, enisa, https://www.enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_pl.pdf [dostęp: 06.09.2023].

Przewodnik wskazuje podobny zakres organizacji procesów cyberbezpieczeństwa jak dokumenty brytyjskie i skupia się na:

- rozwoju kultury cyberbezpieczeństwa;
- przypisaniu zarządom odpowiedzialności za cyberbezpieczeństwo;
- potrzebie uświadomienia pracowników i uzyskania zrozumienia dla konieczności stosowania się do wymagań cyberbezpieczeństwa;
- przeprowadzaniu audytów cyberbezpieczeństwa;
- ochronie danych;
- organizacji szkoleń;
- organizacji współpracy z innymi podmiotami ekosystemu cyberbezpieczeństwa (dostawcami systemów, CERTami);
- opracowaniu planów reagowania na incydenty;
- zabezpieczeniu systemów, urządzeń i sieci.

Poradnik jest publicznie dostępny, ale ponieważ nie jest promowany, to brak podstaw do uznania, że jest często pobierany i wykorzystywany przez polskie małe i średnie firmy. Analiza przeprowadzona na kilku ostatnich stronach poradnika pokazuje, że powszechnie stosowane w Polsce podejście polegające na skupieniu się na rozwoju specjalistycznych zasobów, narzędzi, systemów i specjalistycznych kompetencji oraz rozwoju podstawowej świadomości wymagań cyberbezpieczeństwa potrzebuje rozszerzenia o następujące elementy:

- wpisanie cyberbezpieczeństwa w kontekst funkcjonowania całej organizacji z uwzględnieniem zarządzających i działów operacyjnych;
- budowę kultury cyberbezpieczeństwa i większe skupienie się na użytkownikach systemów;
- dodania do odpowiedzialności za infrastrukturę, dane i systemy komponentu odpowiedzialności za produkty z elementami cyfrowymi w całym cyklu ich użytkowania;
- włączenie kwestii cyberbezpieczeństwa i współpracy w tym zakresie w cały łańcuch wartości.

Warunkiem koniecznym do realizacji tych postulatów jest rozwój kompetencji ogółu specjalistek i specjalistów cyberbezpieczeństwa. Muszą mieć oni odpowiednią wiedzę, umiejętności i pozytywne nastawienie do swoich zadań.

Wymaga to aktualizacji i uzupełnienia kompetencji przynajmniej części specjalistek i specjalistów, którzy już funkcjonują na rynku oraz aktualizacji programów i treści przekazywanych w programach edukacyjnych, co z kolei jest zależne od przygotowania edukatorek i edukatorów do tych zadań oraz treści i narzędzi wykorzystywanych przez nich w procesie edukacji.

MATRYCE KWALIFIKACJI

Jednym z narzędzi do kształtowania programów edukacji i wymagań dla różnych grup specjalistek i specjalistów z zakresu cyberbezpieczeństwa są ramy kwalifikacji i rekomendacje odnośnie do struktury kompetencji dla cybersecurity.

Ramy kompetencji to narzędzia w formie tabel, które pomagają edukatorom oraz różnym organizacjom definiować, opisywać i oceniać kompetencje potrzebne do wykonania określonych zadań. Matryce porządkują i standaryzują opisywane obszary, pozwalają na normalizację języka opisu i ułatwiają edukację i współpracę specjalistów oraz komunikację z szerokimi grupami interesariuszy.

Ramy kompetencji zazwyczaj składają się z następujących elementów:

Definicje kompetencji. Są rozumiane jako kombinacja umiejętności, wiedzy i doświadczenia potrzebnego do wykonania określonego zadania. Zbiór kompetencji danej matrycy określa wymaganą strukturę i szerokość potrzebnych kompetencji w danym obszarze.

Poziomy. Ramy kompetencji zazwyczaj obejmują kilka poziomów kompetencji, od początkującego do eksperta. Poziomy odzwierciedlają różne etapy doświadczenia i umiejętności potrzebnych do wykonania zadania.

Profile. Ramy zawierają i opisują ogół kompetencji w danym obszarze. Do tego ramy często posiadają możliwość nakładania filtrów celem wyboru kompetencji adekwatnych dla określonych ról zawodowych.

Cele wykorzystywania matryc są opisane w raporcie Sektorowej Rady ds. Kompetencji Telekomunikacji i Cyberbezpieczeństwa *Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro*[24], w artykule *Międzynarodowe narzędzia opisu kompetencji cyberbezpieczeństwa – nie wymyślajmy koła od nowa.*

Według tego raportu ramy mogą być używane w:

- tworzeniu opisów stanowisk, zakresów odpowiedzialności i profili ról w obszarze cyberbezpieczeństwa;
- planowaniu docelowych modeli pracy oraz struktur organizacyjnych dla zapewniania cyberbezpieczeństwa;
- planowaniu potrzeb w zakresie zasobów ludzkich w tym obszarze;
- pomocy w pozyskiwaniu i rekrutacji pracowników o odpowiednich umiejętnościach poprzez standaryzację języka opisu i używanie określeń zrozumiałych dla branży i aplikujących specjalistów;
- pomocy w opisie wymagań dla zaangażowania dostawców;
- alokacji pracowników o odpowiednich kompetencjach do odpowiednich zadań i projektów;
- ocenie umiejętności pracowników, dostawców i potencjału organizacji;
- analizie dla projektowania rozwoju kompetencji działu i organizacji;
- rozwoju kompetencji pracowników;
- ustaleniu zasad wynagradzania i szeregowania pracowników w domenie cyberbezpieczeństwa.

Ramy mogę również stanowić punkt odniesienia w tworzeniu i ocenie zakresu programów szkoleniowych.

Stosowanie ram przynosi wymierne korzyści związane z:

- osiągnięciem precyzji opisu kompetencji;
- uzyskaniem i stosowaniem wspólnego języka dla danego ekosystemu;
- zdefiniowaniem koniecznego zakresu zbioru kompetencji, jak i ich struktury i zaawansowania;
- obniżeniem ryzyka w przedsiębiorstwach przez wykorzystanie standardów;
- skróceniem czasu organizacji procesów cyberbezpieczeństwa w przedsiębiorstwie.

24) Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Warszawa 2021.

Do najbardziej popularnych ram kompetencji w obszarze cyberbezpieczeństwa należą:

- **Matryca NICE The Workforce Framework for Cybersecurity** – stworzona przez NIST
- **European Cybersecurity Skills Framework** – opracowana przez ENISA
- **Cyber Career Framework** – przygotowana przez UK Cyber Security Council
- **SFIA 8** – która będąc ramą opisującą szeroki zakres kompetencji potrzebnych dla ról związanych z IT, posiada zakres tematyczny skupiony na cyberbezpieczeństwie; jest ona opracowana przez brytyjską SFIA Foundation.

Matryca NICE The Workforce Framework for Cybersecurity

Prace nad stworzeniem podstawowych narzędzi dla rozwoju kompetencji w zakresie cyberbezpieczeństwa zostały w USA rozpoczęte w 2010 r., kiedy powołano do życia projekt National Initiative for Cybersecurity Education (NICE). Projekt jest partnerstwem publiczno-prywatnym i w jego działanie zaangażowanych jest kilka amerykańskich rządowych agenci oraz uczelnie i firmy sektora prywatnego. Biuro projektu jest umieszczone w strukturach NIST (National Institute of Standards and Technology).

Pierwsza robocza wersja matrycy została opublikowana w 2011 r., a wersja z uwzględnieniem wniosków z szerokich konsultacji została upubliczniona w 2014 r. Celem stworzenia tej matrycy było przyspieszenie rozwoju kompetencji w zakresie cyberbezpieczeństwa poprzez wykorzystanie współpracy pomiędzy sektorem publicznym, uczelniami i branżą, poprawienie i ustrukturyzowanie programów edukacyjnych w zakresie cyberbezpieczeństwa oraz stworzenie narzędzi do planowania zasobów organizacyjnych i rozwoju kariery specjalistek i specjalistów cyberbezpieczeństwa.

Od początku matryca była zorganizowana wokół siedmiu kategorii:

- **SECURELY PROVISION** – zorientowaną na projektowanie i budowę systemów cyberbezpieczeństwa w organizacjach
- **OPERATE AND MAINTAIN** – zorientowaną na utrzymanie i administrowanie systemami
- **PROTECT AND DEFEND** – zorientowaną na identyfikację i zarządzanie ryzykiem
- **INVESTIGATE** – zorientowaną na kontrolę i audyty
- **COLLECT AND OPERATE** – zorientowaną na gromadzenie i przekazywanie do odpowiednich służb informacji o charakterze i źródłach ataków celem przygotowania narzędzi obrony
- **ANALYZE** – zorientowaną na monitorowanie i analizę informacji o działaniu systemów
- **OVERSIGHT AND DEVELOPMENT** – zorientowaną na zarządzanie systemem, współpracę z zarządzającymi organizacjami, planowanie zasobów dla rozwoju systemów cyberbezpieczeństwa, integrację ze strategią firmy, edukację wewnątrz organizacji, wpasowanie w regulacje prawne.

W ramach kategorii identyfikowane były obszary specjalizacji, którym przypisano typowe zadania do realizacji. Następnie do zadań przypisano opisy wymaganej wiedzy i umiejętności.

Ta struktura została utrzymana do dziś z pewnymi drobnymi zmianami w nazwach i zakresie:

- Zmieniono nazwę ANALYZE na INTELLIGENCE
- Zmieniono nazwę SECURELY PROVISION na DESIGN and DEVELOPMENT

- Zmieniono nazwę A OPERATE and MAINTAIN na IMPLEMENTATION and OPERATION
- Zmieniono nazwę COLLECT and OPERATE (CO) na CYBERSPACE EFFECTS (CE)

W wersji wprowadzanej w 2023 r. zmieniono kolejność kategorii. Obecnie wygląda ona następująco:

- OVERSIGHT and GOVERNANCE (OG)
- DESIGN and DEVELOPMENT (DD)
- IMPLEMENTATION and OPERATION (IO)
- PROTECTION and DEFENSE (PD)
- INTELLIGENCE (IN)
- CYBERSPACE EFFECTS (CE)

Ta zmiana wskazuje obszary pod kątem ich prawidłowej kolejności w budowie procesu zapewniania cyberbezpieczeństwa. Dodatkowo podkreśla istotność funkcji organizacyjnych obok technicznych.

Do powyższych kategorii dopasowano również najczęściej występujące role, aby zwiększyć praktyczność wykorzystania ramy i wskazać odniesienia w procesie projektowania organizacji i definiowania struktur i procesów na rzecz cyberbezpieczeństwa.

Rama NICE przypisuje do wszystkich kategorii łącznie 50 ról, z czego najwięcej (16) do kategorii OVERSIGHT and GOVERNANCE, co jest kolejnym argumentem na istotność tej organizacyjnej funkcji. Przypisano jej kilka kategorii ról:

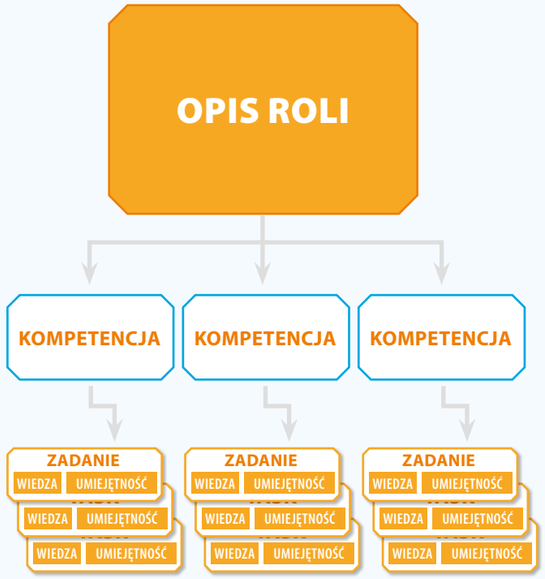
- rozwój organizacji i edukacja pracowników – 3 role
- integracja cyberbezpieczeństwa z funkcjami biznesowymi i zarządczymi – 2 role

- współpraca przy zarządzaniu i realizacji projektów – 2 role
- współpraca i integracja z działami IT – 3 role
- stworzenie i zarządzanie kontrolą – 2 role
- wsparcie prawne dla procesów cyberbezpieczeństwa i prywatności – 2 role
- kwestie zarządzania bezpieczeństwem informacji – 1 rola
- kwestie integracji wymagań cyberbezpieczeństwa w produkty – 1 rola.

Role i zadania z nimi związane dobrze oddają ewolucję i rozwój podejścia do cyberbezpieczeństwa z perspektywy włączenia tej dziedziny w procesy przedsiębiorstwa, rozszerzenia jej wymogów na produkt i jego cykl życia, rozwoju w organizacji odpowiedniej wiedzy i świadomości. W pozostałych kategoriach umieszczono po siedem lub osiem przykładowych ról.

Ramy można używać wykorzystując jedną z dwóch perspektyw:

perspektywa zadaniowa – jest najczęściej wykorzystywana przez firmy i organizacje; wychodzą one od roli zawodowej, przypisanych do niej zadań i potrzebnych do ich realizacji wiedzy i umiejętności;



perspektywę rozwoju wiedzy i umiejętności – wykorzystywana głównie przez edukatorów oraz rozwijających swoje kompetencje w obszarze cyberbezpieczeństwa.

Źródło: https://www.linkedin.com/pulse/overview-nist-nice-framework-cyber-security-training-beyond20/

Rama NICE jest wspierana przez zestaw narzędzi pomagających w jej praktycznym wykorzystaniu. Należą do nich:

- **NICE Framework Mapping Tool**, narzędzie dla działów HR do identyfikacji potrzeb w zakresie cybersecurity
- **Cyber Career Pathways Tool**, narzędzie dla planowania rozwoju i ścieżki kariery dla specjalistów
- **NICCS Education and Training Catalog**, przedstawiający listę programów edukacyjnych odpowiadających wymogom matrycy NICE
- **DHS PushButtonPD™** – narzędzie do szybkiego przygotowywania opisu stanowisk i ogłoszeń rekrutacyjnych dla specjalistów cyberbezpieczeństwa w amerykańskim sektorze publicznym.

W ten sposób tworzony jest cały ekosystem popularyzacji matrycy i ułatwień w jej stosowaniu. Z tych względów rama kompetencji NICE razem z ramą NIST stanowią jedne z najlepszych narzędzi dla organizacji systemów i procesów cyberbezpieczeństwa.

Aktualną ramę NICE można znaleźć w witrynie National Initiative For Cybersecurity Careers And Studies pod adresem:

https://niccs.cisa.gov/workforce-development/nice-framework

MODEL EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

European Cybersecurity Skills Framework została stworzona przez Europejską Agencję Cyberbezpieczeństwa i przedstawiona publicznie we wrześniu 2022 r. Jest więc dokumentem odpowiadającym aktualnym potrzebom. Rama jest adresowana do organizacji, edukatorów, edukatorek, specjalistów i specjalistek oraz osób zainteresowanych pracą w obszarze cyberbezpieczeństwa. Pozycjonowanie to dobrze oddaje poniższa grafika:

Źródło: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Ponadto twórcy ECSF widzą wśród jej odbiorców liderów gospodarczych i politycznych zajmujących się kwestiami kształtowania regulacji i polityk w zakresie cyberbezpieczeństwa oraz wszystkich zainteresowanych tą tematyką[25].

ENISA wskazuje następujące cele swojej matrycy:

- „ECSF zapewnia uzyskanie wspólnej terminologii i sposobów opisu oraz jednolite zrozumienie potrzeb (struktura organizacji, rekrutacja) i profili specjalistów ds. cyberbezpieczeństwa w całej UE (kwalifikacje, szkolenia).
- ECSF wspiera identyfikację kluczowych zestawów umiejętności wymaganych z punktu widzenia oczekiwań względem specjalistek i specjalistów. Umożliwia organizatorom programów edukacyjnych wspieranie rozwoju kluczowych zestawów umiejętności i pomaga decydentom wspierać inicjatywy mające na celu złagodzenie zidentyfikowanych luk w umiejętnościach.
- Rama ułatwia zrozumienie wiodących ról zawodowych w dziedzinie cyberbezpieczeństwa i niezbędnych umiejętności, w tym umiejętności organizacyjnych oraz miękkich, a także aspektów legislacyjnych. W szczególności umożliwia osobom niebędącym ekspertami i działom HR zrozumienie wymagań dotyczących planowania zasobów, rekrutacji i planowania kariery we wspieraniu cyberbezpieczeństwa.
- Rama promuje harmonizację edukacji, szkoleń i rozwoju specjalistów dla zapewniania cyberbezpieczeństwa. Jednocześnie terminologia opisu umiejętności i ról w zakresie cyberbezpieczeństwa dobrze łączy się z terminologią używaną w obszarze opisu kompetencji dla ICT.
- ECSF przyczynia się do osiągnięcia zwiększonej ochrony przed cyberatakami oraz do zapewnienia bezpieczeństwa systemów informatycznych i społeczeństwa. Zapewnia zestandaryzowaną strukturę i rekomendacje dotyczące sposobu budowania zdolności wśród europejskich specjalistów ds. cyberbezpieczeństwa”[26].

Rama jest opisana w dokumencie ECSF EUROPEAN CYBERSECURITY SKILLS FRAMEWORK, umieszczonym w witrynie ENISA pod linkiem:

https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Strukturalnie ECSF różni się nieco od klasycznych ram kwalifikacji, od początku skupia się bowiem na identyfikacji i opisie kluczowych ról występujących w organizacji i realizacji w niej funkcji cyberbezpieczeństwa.

Następnie w ramach roli definiowane są kluczowe dla niej zadania, do realizacji których przypisane są umiejętności oraz potrzebne obszary wiedzy. Dodatkowo do każdej roli dodane są przydatne w jej wykonywaniu kompetencje opisane w matrycy e-competence Framework, stworzonej dla specjalistów branży ICT.

Rama jest dostępna w języku angielskim i nie została dotąd przetłumaczona na język polski. Przykładowy profil przetłumaczony na język polski można jednak znaleźć w publikacji Sektorowej Rady ds. Kompetencji Telekomunikacji i Cyberbezpieczeństwa w artykule *Międzynarodowe narzędzia opisu kompetencji cyberbezpieczeństwa – nie wymyślajmy koła od nowa*[27].

NAZWA PROFILU	MANAGER ZARZĄDZANIA RYZYKIEM CYBERNETYCZNYM
INNE NAZWY PROFILU	• Analityk Ryzyka Bezpieczeństwa Informacyjnego • Konsultant ds. Zapewniania Bezpieczeństwa Cybernetycznego • Konsultant ds. Ryzyk Cyberbezpieczeństwa • Analityk Wpływu Zagrożeń Cybernetycznych • Menedżer Ryzyk Cyberbezpieczeństwa
PODSUMOWANIE ROLI	Zarządza ryzykiem związanym z cyberbezpieczeństwem organizacji w odniesieniu do realizacji jej strategii. Opracowuje, utrzymuje i wdraża procesy zarządzania ryzykiem pochodzącym z zagrożeń cybernetycznych i informacyjnych.
OPIS MISJI	Zarządza (identyfikuje, analizuje, ocenia, szacuje) i odpowiada na ryzyka związane z cyberbezpieczeństwem w zakresie infrastruktury, systemów i usług ICT poprzez planowanie, stosowanie, raportowanie i komunikowanie analizy, oceny i przetwarzania ryzyka. Ustanawia strategię zarządzania ryzykiem dla organizacji i zapewnia, że ryzyko pozostaje na akceptowalnym dla organizacji poziomie poprzez wybór i wdrażanie działań zapobiegawczych i kontrolnych.

25) User Manual European Cybersecurity Skills Framework (ECSF), ENISA, Ateny 2022.

26) European Cybersecurity Skills Framework (ECSF) – https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

27) Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo; Warszawa 2021.

PRZYKŁADOWE REZULTATY	• Raport oceny ryzyka dla cyberbezpieczeństwa • Plan działania na rzecz usuwania ryzyka cybernetycznego
GŁÓWNE ZADANIA	• Opracowanie strategii zarządzania ryzykiem cyberbezpieczeństwa w organizacji • Zarządzanie inwentaryzacją zasobów organizacji • Identyfikacja i ocena zagrożeń i podatności systemów teleinformatycznych związanych z cyberbezpieczeństwem • Identyfikacja krajobrazu zagrożeń, w tym profili atakujących i oszacowanie potencjału ataków • Ocena zagrożeń dla cyberbezpieczeństwa i zaproponowanie najodpowiedniejszych opcji zarządzania ryzykiem, w tym środków kontroli oraz ograniczania i unikania ryzyka w odniesieniu do strategii organizacji • Monitorowanie skuteczności kontroli cyberbezpieczeństwa i poziomów ryzyka • Zapewnienie, że wszystkie zagrożenia dla cyberbezpieczeństwa pozostaną na akceptowalnym poziomie dla organizacji • Opracowanie, utrzymanie, raportowanie i komunikowanie działań pełnego cyklu zarządzania ryzykiem
GŁÓWNE UMIEJĘTNOŚCI	• Umiejętności wdrożenia ram, metodologii i wytycznych dotyczących zarządzania ryzykiem w cyberbezpieczeństwie oraz zapewnienie zgodności z przepisami i standardami • Umiejętności analizy i wykorzystania praktyk zarządzania jakością i ryzykiem w organizacji • Umożliwienie właścicielom procesów i obszarów biznesowych, kadrze kierowniczej i innym interesariuszom podejmowania decyzji ze świadomością ryzyka i możliwością zarządzania nim • Umiejętności budowy środowiska rozumienia ryzyka w zakresie cyberbezpieczeństwa • Umiejętności komunikacji, prezentowania i raportowania do odpowiednich interesariuszy w organizacji • Umiejętności definiowania opcji zarządzania ryzyka
NAJWAŻNIEJSZE OBSZARY WIEDZY	• Zna i rozumie standardy, metodologie i ramy zarządzania ryzykiem • Zna i rozumie narzędzia zarządzania ryzykiem • Zna i rozumie zalecenia i najlepsze praktyki w zakresie zarządzania ryzykiem • Zna i rozumie zagrożenia cybernetyczne • Zna i rozumie luki w zabezpieczeniach systemów komputerowych • Zna zasady kontroli procesów i stosowania rozwiązań w zakresie cyberbezpieczeństwa • Zna i rozumie zagrożenia dla cyberbezpieczeństwa • Zna i rozumie zasady monitorowania, testowania i oceny skuteczności kontroli bezpieczeństwa cybernetycznego • Zna i rozumie zakres korzyści i wykorzystania certyfikatów związanych z cyberbezpieczeństwem • Zna i rozumie technologie związane z cyberbezpieczeństwem
WYMAGANE KOMPETENCJE Z RAMY KOMPETENCJI E-CF	• E.3. Risk Management – poziom 4 • E.5. Process Improvement – poziom 3 • E.7. Business Change Management – poziom 4 • E.9. IS-Governance – poziom 4

ECSF przedstawia szczegółowe opisy 12 kluczowych ról zawodowych dla rozwoju i zapewniania cyberbezpieczeństwa. Każda z nich ujęta jest w jednolity sposób, w oparciu o strukturę przedstawioną w tłumaczeniu opisu roli Manager Zarządzania Ryzykiem Cybernetycznym.

Do 12 opisanych ról w matrycy ECSF należą:

1. CHIEF INFORMATION SECURITY OFFICER (CISO)
2. CYBER INCIDENT RESPONDER
3. CYBER LEGAL, POLICY & COMPLIANCE OFFICER
4. CYBER THREAT INTELLIGENCE SPECIALIST
5. CYBERSECURITY ARCHITECT
6. CYBERSECURITY AUDITOR
7. CYBERSECURITY EDUCATOR
8. CYBERSECURITY IMPLEMENTER
9. CYBERSECURITY RESEARCHER
10. CYBERSECURITY RISK MANAGER
11. DIGITAL FORENSICS INVESTIGATOR
12. PENETRATION TESTER

ECSF definiuje znacznie mniej ról niż rama NICE. Jednak proponowane role pokrywają cały zakres potrzeb i kluczowe obszary zdefiniowane w ramie NICE i zwracają szczególną uwagę na:

- aspekty całościowej organizacji systemu oceny ryzyka i zapewniania cyberbezpieczeństwa (CISO), Cyber Legal Policy & Compliance Officer;
- przygotowanie organizacji z perspektywy świadomości pracowników CS Researcher i CS Educator;
- kwestie włączenia produktów i usług w całym cyklu ich życia w procesy cyberbezpieczeństwa: Cybersecurity Architect, Cybersecurity Auditor;
- zarządzania ryzykiem Cybersecurity Risk Manager;
- przygotowanie systemów: Cybersecurity Implementer, Penetration Tester;
- odpowiedzi na ataki: Cyber Incident Responder;
- zbierania informacji i współpracy z innymi funkcjami ekosystemu cyberbezpieczeństwa: Digital Forensic Investigator, Cyber Threat Intelligence Specialist.

Dzięki takiemu podejściu rama ECSF ma potencjał do jej łatwego wykorzystania, chociaż z pewnością na drodze ku temu stoi jej krótka historia, brak tłumaczenia na język polski i brak działań promocyjnych ze strony ENISY i innych instytucji zaangażowanych w organizację i rozwój ekosystemu na rzecz wspierania cyberbezpieczeństwa w Polsce.

Przetłumaczona rama ECSF z pewnością powinna znaleźć się w zasobach NASK i być promowana przez instytucje zajmujące się edukacją na rzecz przygotowania specjalistów cyberbezpieczeństwa.

RAMA CHARTERED INSTITUTE OF INFORMATION SECURITY (CIISEC)

Jedną z pierwszych ram dla rozwoju kompetencji w obszarze cyberbezpieczeństwa przygotowano w brytyjskim Institute of Information Security Professionals, który został w 2018 r. przemianowany na Chartered Institute of Information Security[28]. W 2007 r. Instytut opublikował ramę przeznaczoną do rozwijania kompetencji w obszarze cyberbezpieczeństwa. W listopadzie 2019 r. opublikowano

28) CIISEC – https://www.ciisec.org/.

jej wersję 2.4 (CIISec Skills Framework). Prezentuje ona zarówno klasyczne podejście z perspektywy opisu kompetencji poprzez umiejętności i wiedzę, jak i bezpośrednio odnosi się do zdefiniowanych ról zawodowych. Kompetencje są umieszczone w 11 grupach:

1. Information Security Governance and Management
2. Threat Assessment and Information Risk Management
3. Implementing Secure Systems
4. Assurance: Audit, Compliance and Testing
5. Operational Security Management
6. Incident management, Investigation and Digital Forensics
7. Data Protection, Privacy and Identity Management
8. Business Resilience
9. Information Security Research
10. Management, Leadership, Business and Communications
11. Contributions to the Information Security Profession and Professional Development.

W każdej z grup znajduje się po kilka kompetencji, które mogą występować na jednym z sześciu poziomów: od 1– *Basic Knowledge* do 6 – *Principlal/Lead Practitioner*.

Rama zawiera także odniesienie do ról zawodowych celem ułatwienia korzystania z jej zasobów.

Rama definiuje następujące role zawodowe w obszarze cybersecurity:

1. Chief Information Security Officer (CISO)
2. Head of Cyber/Information Security
3. Information Security Risk Manager
4. Information Security Risk Officer
5. System Security Manager
6. ComSec Manager
7. Senior Security Architect
8. Technical Security Architect
9. Pen Tester
10. Threat Analyst
11. Vulnerability Analyst

Odniesienia do tej ramy i jej elementy są wykorzystywane w kolejnej brytyjskiej ramie promowanej przez UK Cyber Security Council.

UK CYBER SECURITY COUNCIL CYBER CAREER FRAMEWORK

W ramach swoich prac UK Cyber Security Council opracowała zestaw konkretnych rekomendacji dotyczących rozwoju kompetencji cyberbezpieczeństwa, tworząc UK Cyber Security Council Cyber Career Framework.

Brytyjską ramę można znaleźć pod adresem: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/

Podobnie jak w przypadku ramy NICE i ECSF, UKCSC zorganizowała swoją ramę z perspektywy ról zawodowych i zdefiniowała 16 specjalizacji w zakresie cyberbezpieczeństwa.

Każda z tych ról jest opisana wg następującej struktury:

- ogólny opis roli;
- zakres odpowiedzialności i główne zadania do realizacji;
- wymagana wiedza – z wymienieniem poszczególnych obszarów i bezpośrednim ich powiązaniem z CyBOK;
- wymagane umiejętności, które są podzielone na kilka obszarów:
- obszar umiejętności ogólnych, związanych z organizacją, komunikacją, zarządzaniem procesami i – jeśli potrzebne – z zarządzaniem ludźmi;
- obszar umiejętności specjalistycznych z zakresu cyberbezpieczeństwa;
- dodatkowo wymagane umiejętności są odniesione do ramy Chartered Institute of Information Security (CIISec);
- w tej części jest również opisane doświadczenie, jakie jest potrzebne do wykonywania danej roli;
- ścieżka kariery i powiązane role, dające możliwość planowania rozwoju i kariery w średniej i dłuższej perspektywie;
- certyfikaty – ta część jest w dalszym ciągu rozwijana i ma w założeniu odnosić się do formalnych certyfikatów, akredytacji poświadczających uzyskanie określonych kompetencji.

Ze względu na swój przekrojowy charakter i liczne odniesienia, rama ta jest bardzo przydatna i praktyczna. Dobrze pokazuje zależności pomiędzy rolami, odnosi się do innych narzędzi i zasobów oraz wskazuje specjalistom perspektywę dalszego rozwoju.

Rama UK Cyber Security Council Cyber Career Framework jest uzupełniona o dodatkowe narzędzia takie jak:

- **Career mapping tool** – z ankietą pozwalającą na dobór adekwatnych szkoleń;
- odniesienie do dostępnych programów szkoleniowych i do obecnych programów uzyskiwania certyfikacji technicznych.

Pozwala to na jej stosowanie w pełniejszym kontekście, a dodatkowe narzędzia nadają jej większą, praktyczną wartość

STRUKTURA OPISU ROLI W RAMIE UK CYBER SECURITY COUNCIL CYBER CAREER FRAMEWORK

Working life
An introduction to this specialism

Responsibilities
What will your responsibilities include?
What are you tasks likely to include?

Skills
What personal attributes might you need?
What specialist skills are important?

Knowledge
What core, related and wider knowledge is important for working in this specialism?

Moving on
What other cyber security or IT role might you progress to from this specialism?

Qualifications
Which certifications and qualifications are relevant to roles in this specialism?

SFIA – SKILLS FRAMEWORK FOR THE INFORMATION AGE

Rama SFIA została przygotowana przez brytyjską Fundację Skills Framework for the Information Age. Liderem prowadzącym prace fundacji jest British Computer Society. Fundacja działa od roku 2000 i zajmuje się tworzeniem ram kompetencji dla profesjonalistów całego segmentu ICT. Prace nad ramami kompetencji były prowadzone przez konsorcjum 30 organizacji i instytucji. Był to wysiłek podjęty przez samą branżę, bez bezpośredniego udziału agend rządu Wielkiej Brytanii.

Fundacja do tej pory przygotowała osiem wersji ramy SFIA. Pierwsza została opracowana w 2000 r., a aktualna wersja 8.0 została opublikowana we wrześniu 2021 r. Obecnie w zaawansowanych konsultacjach jest już kolejna, dziewiąta edycja ramy, której oficjalną publikację wstępnie zaplanowano na drugą połowę 2024 r.

Rama jest wykorzystywana w 180 krajach, co czyni ją jednym z najpopularniejszych narzędzi dla wsparcia rozwoju kompetencji IT. Daje szerokie wsparcie w ekosystemie edukacyjnym, IT i konsultingowym oraz jest używana do definiowania strategii i polityk rozwoju branży.

Ogólna struktura ramy

Strukturalnie SFIA jest klasyczną formą ramy kompetencji, do której dodane są elementy ułatwiające jej praktyczne wykorzystanie w wielu obszarach i wielu wymiarach. Opisuje 121 kompetencji, które są umieszczone w siedmiu grupach. W praktyce mamy do dyspozycji prawie 500 opisów kompetencji przypisanych do odpowiednich poziomów zaawansowania.

Rama dzieli kompetencje specjalistów IT na sześć głównych kategorii:

1. Strategy and architecture (Strategia i architektura)
2. Change and transformation (Zarządzanie zmianą i transformacja)
3. Development and implementation (Rozwój i wdrożenia)
4. Delivery and operation (Wykorzystywanie i Utrzymanie)
5. People and skills (Zarządzanie Ludźmi i Rozwój Kompetencji)
6. Relationships and engagement (Sprzedaż, Marketing i Zarządzanie Łańcuchem Dostaw)

W kategoriach zdefiniowane są bardziej szczegółowe podkategorie, w ramach których są umieszczone konkretne kompetencje techniczne.

Oprócz kompetencji technicznych rama definiuje kompetencje ogólne (*business skills*), takie jak: komunikacyjne, organizacja pracy własnej, zarządzanie własną edukacją i rozwojem osobistym, podejmowanie decyzji, umiejętność współpracy, ustrukturyzowane rozwiązywanie problemów, korzystanie z podstawowych narzędzi cyfrowych.

Zakres tych ogólnych kompetencji obejmuje więcej obszarów niż kompetencje społeczne i ważne kompetencje zorientowane na pracę współpracę i pracę w grupie, bo obejmują również grupę kompetencji poznawczych związanych z krytycznym myśleniem, elastycznością poznawczą i rozwiązywaniem problemów.

Każda kompetencja, zarówno techniczna, jak i biznesowa, może występować na jednym z siedmiu poziomów zaawansowania wymagań i odpowiedzialności. Rosną one od poziomu najniższego (1) do najbardziej zaawansowanego (7). Nie każda kompetencja ma wymagania zdefiniowane na każdym poziomie.

Definicje poziomów są określone w następujący sposób:

- **Follow** – pracuje pod bieżącą kontrolą, wykonując ściśle bieżące polecenia;
- **Assist** – pracuje z rutynowym poziomem kontroli, potrafi samodzielnie oceniać, kiedy wymaga dodatkowej pomocy;
- **Apply** – pracuje z ograniczonym poziomem kontroli, współpracuje z innymi, rozumie rezultaty, które ma dostarczyć;
- **Enable** – pracuje z minimalnym poziomem kontroli w oparciu o zdefiniowany zakres odpowiedzialności, współpracuje aktywnie w organizacji i z zewnętrznymi podmiotami;
- **Ensure, advise** – pracuje w oparciu o zdefiniowane ogólne kierunki zadań samodzielnie definiując zakres pracy; samodzielnie podejmuje decyzje, wpływa na pracę innych osób w organizacji i poza nią; rozwiązuje złożone problemy i realizuje działania o charakterze strategicznym; organizuje pracę zespołów i współpracę pomiędzy różnymi zespołami;
- **Initiate, influence** – posiada szeroki zakres uprawnień do podejmowania decyzji i kształtowania kierunków i zakresu pracy dużych komórek organizacyjnych; współpracuje z najwyższym poziomem organizacji; podejmuje istotne decyzje o wymiarze finansowym; wyznacza kierunki rozwoju organizacji; posiada szeroki zakres kompetencji zarządczych;
- **Set strategy, inspire, mobilise** – ponosi pełną odpowiedzialność za organizację i jej efekty; definiuje strategie i sposoby alokacji i wykorzystywania zasobów; wpływa na branżę i otoczenie organizacyjne; kształtuje organizację; posiada szeroki zakres kompetencji liderskich i zarządczych.

Dodatkowo rama definiuje trzy kolejne wymiary, które są przypisywane roli zawodowej. Te wymiary to:

1. **Autonomy** – Poziom autonomii
2. **Influence** – Poziom wpływu
3. **Complexity** – Umiejętność radzenia sobie ze złożonymi sytuacjami

Każdy z tych wymiarów funkcjonuje na jednym z siedmiu opisanych wyżej poziomów.

Końcowym elementem uzupełniającym powyżej opisane wymagania jest definicja zakresu wiedzy, jaka jest niezbędna do realizacji wybranych wymagań. SFIA często odnosi się do skodyfikowanych opisów wiedzy zwanych Body of Knowledge (BOK). SFIA odnosi się do kilkudziesięciu kodeksów wiedzy przypisanych do poszczególnych kategorii kompetencji zawodowych. Do przykładowych kodeksów (BOK) należą:

- **DPBOK** – Digital Practitioner Body of Knowledge
- International Risk Management Standards
- **CYBOK** – Cybersecurity
- **PMBOK** – Project Management
- **SABOK** – Systems Administration
- **SWEBOK** – Software Engineering
- NIST Framework

Wszystkie behawioralne wymagania względem poszczególnych poziomów są uporządkowane i opisane w odrębnym dokumencie[29].

Wymagania potrzebne do opisania kompetencji konkretnej roli zawodowej składają się więc ze złożenia i opisania następujących elementów:

- opisu wybranych dla roli kilku kompetencji technicznych z dobranymi, odpowiednimi poziomami wymagań;

29) Glossary Of Behavioural Factors Within The 7 Levels Of Responsibility (24 września 2021), SFIA Foundation, https://sfia-online.org/en/assets/sfia-behavioural-factors/sfia-v8-levels-of-responsibility-behavioural-factors-glossary_original-final_24-sept-2021.pdf [dostęp: 6.09.2023].

- dobranym poziomem kompetencji biznesowych;
- dobranymi poziomami dodatkowych wymiarów autonomii, wpływu i radzenia sobie ze złożonymi wyzwaniami;
- przypisaniem wymaganego zakresu wiedzy.

Stworzenie takiej wszechstronnej struktury dla opisu kompetencji jest niezwykle użyteczne, ponieważ pokazuje cały szereg współzależności pomiędzy różnymi ich obszarami. Wiąże je z konkretnymi wymogami odnoszącymi się do wymiarów autonomii, wpływu i zarządzania złożonością oraz kompetencjami umieszczonymi w grupie *business skills*, gdzie mieszczą się również kompetencje społeczne. Dodatkowo rama zwraca uwagę na kompetencje współpracy i organizacji pracy. Rama SFIA jest jedną z nielicznych, które precyzyjnie definiują wymagania względem wszystkich trzech kluczowych grup kompetencji potrzebnych dla nowoczesnej gospodarki:

- technicznych i cyfrowych
- poznawczych
- społecznych, w tym zorientowanych na współpracę.

W celu ułatwienia praktycznego wykorzystania ram zostały przygotowane wybrane profile odnoszące się do konkretnych obszarów. Ich stosowanie przynosi szereg konkretnych korzyści:

- wstępnie definiują zakresy kompetencji z perspektywy dopasowania do danego obszaru
- skracają czas potrzebny na selekcjonowanie wymaganych kompetencji
- określają kluczowe zależności pomiędzy różnymi kompetencjami wymaganymi dla danego obszaru
- tworzą kontekst dla funkcjonowania ról biznesowych.

Zdefiniowane profile w ramach SFIA to:

- Digital Transformation skills view
- Agile skills view
- DevOps skills view
- Big Data/Data Science skills view
- Information and cyber security skills view
- Enterprise IT view.

Warto zwrócić uwagę na szeroki zakres zdefiniowanych profili. SFIA jest zorientowana na klasyczny rdzeń kompetencji IT (Enterprise IT view), ukierunkowanych na nowoczesne podejście do rozwoju projektów cyfrowych i tworzenia oprogramowania (Agile i DevOps skills). Oprócz tego kładzie nacisk na kompetencje dla kluczowych obszarów stosowania technologii, jak wykorzystanie danych (Big Data/Data Science/AI), cyberbezpieczeństwo i bezpieczeństwo informacji (Information and cyber security skills) oraz transformację cyfrową (Digital Transformation skills). Na potrzeby tej analizy skupimy się na perspektywie cyberbezpieczeństwa.

SFIA – perspektywa Information and cyber security skills

Perspektywa Information and *cyber security skills* pojawiła się w najnowszej, ósmej wersji ramy i jest cały czas rozwijana. Punktem wyjścia do opracowania tej perspektywy było zdefiniowanie operacyjnego modelu zarządzania ryzykiem i zapewniania cyberbezpieczeństwa w organizacji. Model zawiera klarownie sformułowane i komunikowane podstawowe założenia:

- cyberbezpieczeństwo i zarządzanie bezpieczeństwem jest wbudowane w kulturę całej organizacji na każdym etapie jej rozwoju;

- liderki i liderzy są wzorem do naśladowania wymaganych zachowań w zakresie cyberbezpieczeństwa i odgrywają bardzo istotną rolę w budowie i funkcjonowaniu całego systemu;
- realizacja funkcji bezpieczeństwa jest ogólnie akceptowaną częścią codziennej pracy i praktyk zarządzania;
- funkcje bezpieczeństwa mają być wbudowane w procesy, usługi i produkty by-design i w sposób domyślny (by-default), a nie jako dodatkowy uzupełniający element dodany po fakcie.

Każdemu elementowi modelu operacyjnego cyberbezpieczeństwa można przypisać konkretne odpowiedzialności i wymagania z perspektywy zarządzania ryzykiem i zapewnieniem cyberbezpieczeństwa. Do realizacji tych wymagań należy dobrać wykonawców, osoby z odpowiednimi umiejętnościami, wiedzą i kompetencjami oraz odpowiednimi poziomami zaawansowania.

Do każdego elementu opisanego w modelu zdefiniowano zakres odpowiedzialności i przypisano kluczowe kompetencje. Są one już wcześniej określone w ramie i występują również w opisach kwalifikacji ICT.

Prace nad definicją finalnego zakresu tych kompetencji jeszcze trwają. Dotąd w ramach prac analitycznych i konsultacyjnych dokonano mapowania kompetencji z ram NIST i NICE z SFIA *Information and cyber security skills* oraz zdefiniowano listę tych, które należy zweryfikować pod kątem uzupełnienia o perspektywę cyberbezpieczeństwa. Na tej liście znajdują się obecnie następujące kompetencje:

- **BURM** – Business Risk Management
- **COPL** – Continuity Management
- **GOVN** – Enterprise IT Governance
- **INAS** – Information Assurance
- **IRMG** – Information Governance
- **ITCM** – Contract Management
- **ITOP** – IT Infrastructure
- **OCDV** – Organisational Capability Development
- **PENT** – Penetration Testing
- **RLMT** – Relationship Management
- **SCAD** – Security Administration
- **SUPP** – Supplier Management
- **USUP** – Incident Management

W efekcie przykładowy opis elementu modelu operacyjnego dla cyberbezpieczeństwa wygląda tak:

ELEMENT OPERACYJNEGO MODELU BEZPIECZEŃSTWA	Odpowiedzialności odnoszące się do zarządzania ryzykiem i zapewniania cyberbezpieczeństwa	Przypisane kompetencje z matrycy SFIA	Powiązania z działaniami specjalistów cyberbezpieczeństwa
PROCUREMENT/ SUPPLIER MANAGEMENT ZAKUPY I ZARZĄDZANIE DOSTAWCAMI	Zarządzanie dostawcami np. usług chmurowych, aplikacji, systemów ERP Zarządzanie komunikacją z dostawcami • zapytania, procesy zakupowe Ocena ryzyka w łańcuchu dostaw Due diligence kontraktów i umów Coroczna ocena dostawców	Sourcing **SORC** Supplier management **SUPP** Continuity planning **COPL** Contract management **ITCM** Relationship management **RLMT**	Specjaliści ds. zakupów i zarządzania dostawcami są odpowiedzialni za codzienne czynności związane z zapewnianiem bezpieczeństwa, monitorowanie i raportowanie w oparciu o wymagania ram bezpieczeństwa Specjaliści zakupów i zarządzania dostawcami integrują wymagania bezpieczeństwa z praktykami zarządzania zaopatrzeniem i dostawcami Specjaliści ds. cyberbezpieczeństwa mają nadzór nad ich pracami w celu zapewnienia bezpieczeństwa Specjaliści ds. bezpieczeństwa udzielają porad, wskazówek i wsparcia w zarządzaniu zaopatrzeniem i dostawcami

Kluczowym elementem jest tutaj powiązanie z opisami poszczególnych kompetencji SFIA. Poniżej przedstawiamy przykładowy opis jednej z kompetencji Continuity management COPL (zapewnianie ciągłości biznesowej):

CONTINUITY MANAGEMENT COPL	Rozwój, wdrożenia, testowanie i utrzymanie działań zapewniających ciągłość prowadzenia operacji biznesowych *Developing, implementing and testing a business continuity framework*

OGÓLNE WSKAZANIA	Działania mogą obejmować (ale nie są ograniczone): • identyfikowanie potencjalnych zagrożeń i ocenę ich wpływu na działalność biznesową • tworzenie planów i procedur reagowania na incydenty • zapewnienie, że krytyczne funkcje biznesowe mogą kontynuować działalność przy planowanym poziomie zakłóceń • zapewnienie, że akceptowalny poziom usług może zostać przywrócony po wystąpieniu zakłóceń • rozwijanie odporności organizacyjnej • upewnienie się, że ciągłość jest uwzględniana w systemach, procesach i sposobach pracy • wdrażanie praktyk zarządzania ciągłością działania dla usług opartych na chmurze • ciągłe dostarczanie, wdrażania i integracja aplikacji i infrastruktury bez niekorzystnego wpływu lub zakłóceń w usłudze Incydenty mają różnorodne przyczyny, w tym między innymi: cyberataki, naruszenia danych, działania przestępczości zorganizowanej, pożary, powodzie, klęski żywiołowe, pandemie, wystąpienie nagłych sytuacji zdrowotnych i zaburzenia łańcucha dostaw
POZIOMY ZAAWANSOWANIA WYMAGAŃ	
POZIOM 2	Prowadzi rejestr wszystkich działań związanych z zapewnianiem ciągłości, w tym związanych z testami i szkoleniami oraz zapewnia dostępność całej dokumentacji Rejestruje podejmowane działania oraz ich konsekwencje po incydencie lub po przetestowaniu planu zapewniania ciągłości działania w celu stworzenia raportu z wnioskami i zaleceniami
POZIOM 3	Stosuje zorganizowane podejście do opracowania i udokumentowania szczegółów planu zapewniania ciągłości działania Prowadzi dokumentację planów zapewniania ciągłości działania i planów przywracania ciągłości po poważnym incydencie Wspiera opracowywanie planu testowania
POZIOM 4	Wspiera opracowywanie planów zarządzania ciągłością działania Identyfikuje systemy informatyczne i komunikacyjne, które obsługują kluczowe procesy biznesowe Koordynuje analizę wpływu na działalność biznesową i ocenę ryzyka Koordynuje planowanie, projektowanie i testowanie planów awaryjnych
POZIOM 5	Zarządza opracowywaniem, wdrażaniem i testowaniem planów zarządzania ciągłością działania Zarządza relacjami z osobami i zespołami, które mają uprawnienia w ramach działania kluczowych procesów biznesowych i systemów wsparcia Ocenia kluczowe ryzyka i identyfikuje obszary priorytetowe do poprawy Testuje plany zarządzania ciągłością działania i procedury, aby upewnić się, że skutecznie reagują na zagrożenia i że uzgodniony poziom ciągłości może być utrzymany

POZIOM 6	Określa strategię zarządzania ciągłością działania w całej organizacji Zabezpiecza zaangażowanie organizacji, finansowanie i zasoby na potrzeby zarządzania ciągłością działania Kieruje ćwiczeniami zarządzania ciągłością działania Komunikuje politykę, strukturę zarządzania, zakres i role związane z zarządzaniem ciągłością działania. Posiada określone uprawnienia i odpowiedzialność za działania i decyzje związane z zarządzaniem ciągłością działania

Twórcy ramy podkreślają, że ma ona dotyczyć umiejętności, wiedzy i kompetencji potrzebnych do wykonywania określonego zakresu pracy, a nie odnosi się do wąsko zdefiniowanego opisu stanowiska. Opisy stanowisk zależą od konkretnej realizacji struktury organizacyjnej.

Jednak twórcy ramy, rozumiejąc potrzebę praktycznego jej wykorzystania, publikują listę przykładowych funkcji pokrywających obszar zarządzania cyberbezpieczeństwem i umieszczają na tej liście następujące role:

1. Cyber Security Analyst
2. Cyber Security Architect
3. Cyber Security Engineer
4. Cyber Security Instructor
5. Cybers Security Manager
6. Cyber Security Project Manager
7. Cyber Security Technician
8. Cyber Security Researcher
9. DevSecOps Developer
10. Forensic Computer Analyst
11. Security Consultant
12. Incident Responder
13. Penetration Tester
14. Risk Adviser
15. Security and Compliance Auditor.

Jest to dosyć standardowa lista, warto jednak podkreślić wyszczególnienie kilku ról bezpośrednio odnoszących się do kwestii pełnej integracji funkcji cyberbezpieczeństwa z procesami organizacji. Z tej perspektywy warto wyróżnić umieszczenie na tej liście takich ról jak:

- Cyber Security Instructor
- Cyber Security Researcher
- DevSecOps Developer
- Security Consultant.

SFIA jest jedną z najlepiej rozwiniętych ram kompetencji. Posiada szeroką listę dodatkowych narzędzi, które ułatwiają jej stosowanie.

Rama oferuje również szerokie wsparcie różnym grupom odbiorców. Chociaż prace nad profilem *Information and cyber security skills* nie są jeszcze w pełni ukończone, to jest to jedno z najlepszych narzędzi i warto śledzić jego dalszy rozwój.

SEKTOROWE RAMY KWALIFIKACJI W POLSCE

W Polsce tworzenie ram kompetencji jest wspierane przez Instytut Badań Edukacyjnych i Sektorowe Rady ds. Kompetencji. Obszarem cyberbezpieczeństwa zajmuje się Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo. Jest to również obszar pokrewny do działań Sektorowej Rady ds. Kompetencji Informatyka.

W obszarze telekomunikacji, cyberbezpieczeństwa i IT opublikowano dotąd dwie ramy kwalifikacji. Sektorowa Rama Kwalifikacji dla Sektora Telekomunikacyjnego w Polsce (SRK Tele)[30] została opublikowana w lutym 2015 r. i odnosi się do dwóch obszarów kompetencji wymaganych przez sektor telekomunikacji:

- budownictwa telekomunikacyjnego, instalacji, montażu i serwisu urządzeń telekomunikacyjnych;
- sprzedaży usług telekomunikacyjnych i obsługi klienta w różnych segmentach rynku oraz zakupów, sprzedaży i logistyki w obszarze usług dla przedsiębiorców telekomunikacyjnych.

Rama ta nie odnosi się do obszaru cyberbezpieczeństwa.

Sektorowa rama kwalifikacji dla sektora informatycznego w Polsce (SRK IT)31 skupia się na opisie dwóch kompetencji: administrowania i programowania.

W opisach kompetencji administrowania pojawia się kilka odniesień do cyberbezpieczeństwa:

- Na poziomie 4 znajdziemy wymaganie związane z umiejętnościami: „potrafi zabezpieczyć dane, sprzęt i oprogramowanie pojedynczego urządzenia osobistego i mobilnego".
- Na poziomie 5 w obszarze wiedzy powiązanej z administrowaniem jest wymaganie: „zna i rozumie zagrożenia związane z przestępczością elektroniczną".
- Na poziomie 6 w kompetencji administrowanie umieszczone jest wymaganie: „potrafi planować wydajność i bezpieczne wykorzystanie wirtualnego środowiska pracy w przechowywaniu i przetwarzaniu danych".
- Na poziomie 7 kompetencji administrowanie włączone jest wymaganie: „zna i rozumie rodzaje zagrożeń dla bezpieczeństwa oraz ciągłości działania systemów informatycznych" oraz „potrafi zarządzać dużymi i zróżnicowanymi zespołami, stosując jedną ze znanych metodyk zarządzania projektem lub zarządzania procesami, uwzględniając zarządzanie ryzykiem, poszukiwanie nowych rozwiązań oraz jakość i efektywność ekonomiczną prowadzonych prac, zaplanować zabezpieczenie danych i systemów na wysokim poziomie, stosownie do wymagań ekonomicznych, prawnych, spodziewanych zagrożeń i dostępnych technologii".

Te nieliczne odniesienia do zapewniania cyberbezpieczeństwa nie mają charakteru całościowego i nie mają związku z żadnym ze standardów definiujących zakres, wymagania i kompetencje potrzebne dla zarządzania ryzykiem i zapewniania cyberbezpieczeństwa.

Obecnie w Instytucie Badań Edukacyjnych prowadzone są prace związane z przygotowaniem ramy kwalifikacji dla cyberbezpieczeństwa i należy mieć nadzieję, że w toku tych prac powstanie dokument odzwierciedlający rozwój sektora oraz biorący pod uwagę podstawowe standardy i narzędzia wykorzystywane w branży cyberbezpieczeństwa na świecie.

30) Sektorowa rama kwalifikacji. Dla sektora telekomunikacyjnego w Polsce (luty 2015), Kapitał Ludzki, IBE, UE, https://kwalifikacje.edu.pl/wp-content/uploads/publikacje/PDF/srk/SRKTele.pdf [dostęp: 06.09.2023].
31) Sektorowa rama kwalifikacji. Dla sektora informatycznego w Polsce, Ludzki, IBE, UE, http://www.krk-www.ibe.edu.pl/download/ramy_polska/it/SRKIT.pdf [dostęp: 06.09.2023].

PODSUMOWANIE

Cyberbezpieczeństwo jest dziedziną, która rozwija się tak szybko jak cyfryzacja gospodarki, sektora publicznego i wszystkich innych dziedzin naszego życia. Do istotnych trendów, które są widoczne w rozwoju cyberbezpieczeństwa, a które mają istotny związek z wymaganiami kompetencyjnymi należy obecnie zaliczyć:

1. Całościowe podejście do kwestii zapewniania bezpieczeństwa i integracja działań związanych z cyberbezpieczeństwem, zapewnianiem bezpieczeństwa informacji i bezpieczeństwa rozproszonej, podłączonej do sieci komunikacyjnych infrastruktury.

2. Pełne włączenie wymogów cyberbezpieczeństwa we wszystkie procesy biznesowe w organizacji i wzrost roli zarządzania tą dziedziną.

3. Zaangażowanie kierownictwa organizacji, z włączeniem najwyższych szczebli, w procesy zarządzania ryzykiem i zapewnianiem cyberbezpieczeństwa.

4. Rozszerzenie działań związanych z cyberbezpieczeństwem na produkty i usługi, które zawierają elementy cyfrowe oraz włączenie w obszar zapewniania cyberbezpieczeństwa całego cyklu życia produktów i usług.

5. Pogłębiającą się specjalizację rozwiązań cyberbezpieczeństwa w poszczególnych branżach na skutek rozwoju Internetu Rzeczy.

6. Postępujące włączanie kluczowych wymagań cyberbezpieczeństwa w regulacje prawne i wzrost skali raportowania i realizacji konkretnych obowiązków związanych z zarządzaniem ryzykiem i zapewnianiem cyberbezpieczeństwa.

Odzwierciedlenie tych trendów jest widoczne we wzroście odpowiedzialności rządów wielu państw za stymulowania rozwoju i koordynację ekosystemu cyberbezpieczeństwa. Dobry przykład takiego podejścia znajdziemy szczególnie w Wielkiej Brytanii.

Także Unia Europejska aktywnie działa na rzecz integracji i harmonizacji podejścia do cyberbezpieczeństwa krajów członkowskich poprzez stosowne regulacje.

Wszystkie aktualizacje wymagań cyberbezpieczeństwa i ram kompetencji akcentują zwiększenie wagi kwestii zarządczych i integracji cyberbezpieczeństwa z wszystkimi procesami firmy. Proponowana zmiana ikonicznej matrycy NIST z dołożeniem horyzontalnej funkcji zarządzania (Govern) jest tu najlepszym przykładem.

Wszystkie kraje mierzą się obecnie z niedoborem specjalistów cyberbezpieczeństwa i z koniecznością rozwijania systemów ich edukacji. Dlatego oczywisty jest powszechny nacisk na rozwój ram kompetencji, które będą referencjami i zaleceniami dla edukatorów i firm w zakresie przygotowania programów rozwoju kompetencji dotyczących cyberbezpieczeństwa.

W rozwoju takich programów edukacyjnych istotne staje się otwarcie tradycyjnie zorientowanej na kwestie techniczne branży na dodatkowy obszar kompetencji dotyczących zarządzania, wiedzy branżowej, zarządzania ryzykiem i bezpieczeństwem całej organizacji.

Mocno widoczny jest też nacisk na budowę narzędzi ułatwiających wykorzystanie ogólnych ram kompetencji przy definiowaniu ról zawodowych związanych z cyberbezpieczeństwem i precyzyjnym definiowaniem wymogów dla tych ról. Taką drogą poszła ENISA, NIST z matrycą NICE oraz brytyjskie NCSC.

Bardziej szczegółowe rekomendacje zostały umieszczone w kolejnej części tego opracowania.

REKOMENDACJE W SPRAWIE PROGRAMÓW EDUKACYJNYCH DLA CYBERBEZPIECZEŃSTWA

WSTĘP

Dodatkowo postępująca integracja funkcji cyberbezpieczeństwa z większością procesów w organizacji i uwzględnienie bezpieczeństwa usług i produktów w zakresie odpowiedzialności cyberbezpieczeństwa zmieniają strukturę koniecznych dla tego obszaru kompetencji.

Postępujące wpisywanie odpowiedzialności za rezultaty działań związanych z zarządzaniem ryzykiem i zapewnianiem bezpieczeństwa w regulacje prawne podnosi poprzeczkę oczekiwań wobec jakości programów edukacyjnych i skuteczności działania przygotowywanych w nich specjalistów.

Rosnący popyt na specjalistki i specjalistów tworzy warunki do szybkiego wzrostu podaży programów edukacyjnych, co często nie daje gwarancji ich wysokiej jakości ze względu na brak odpowiednio przygotowanych edukatorek i edukatorów oraz presję rynku na nowe kadry.

Kombinacja tych czynników stawia wiele trudnych wyzwań przed tworzącymi programy edukacyjne w zakresie cyberbezpieczeństwa. Dlatego tym opracowaniem chcemy im pomóc w ich misji, a w szczególności:

- uwzględnić wszystkie kluczowe trendy w zakresie rozwoju cyberbezpieczeństwa
- skrócić czas przygotowania programów edukacyjnych
- sformułować wymagania związane z niezbędnym zakresem tych programów, w tym listę zagadnień oraz opis poszczególnych kompetencji
- dać podstawy do formułowania oczekiwać względem wykładowców
- wskazać odniesienia do kluczowych standardów cyberbezpieczeństwa
- ułatwić aktualizację i utrzymanie jakości programów edukacyjnych
- podpowiedzieć narzędzia zwiększające efektywność oferowanej wiedzy i umiejętności praktycznych
- wskazać bezpośrednie źródła know-how w zakresie rozwoju kompetencji cyberbezpieczeństwa w postaci wiodących ram kompetencji i narzędzi ułatwiających ich stosowanie.

ROLE I KOMPETENCJE W GŁÓWNYCH PROCESACH ZAPEWNIANIA CYBERBEZPIECZEŃSTWA

Wraz z postępującą cyfryzacją i nasyceniem elementami cyfrowymi większości produktów i usług rośnie ich podatność na zagrożenia cybernetyczne. Rozszerzające się połączenia między różnymi systemami zwiększają ich współzależność i otwierają nowe obszary ryzyka.

Większość organizacji zdaje sobie sprawę z rosnącej skali ryzyka i przykłada większą wagę do tworzenia systemów zorientowanych na zapewnianie ciągłości swoich operacji. Ale ciągłość ta może być zakłócona przez wiele czynników, wśród których przybywa tych związanych z zagrożeniami cybernetycznymi.

Z punktu widzenia celów organizacji kluczową kwestią jest utrzymanie ciągłości działania, do czego potrzebne jest całościowe podejście do zapewniania bezpieczeństwa. Składa się na nie cyberbezpieczeństwo, bezpieczeństwo informacji i bezpieczeństwo fizyczne. Dlatego korzystne jest odniesienie zakresu programów edukacyjnych w obszarze cyberbezpieczeństwa do standardu ISO/EIC 2700132, który takie systemowe podejście oferuje.

Kolejną zaletą tworzenia programów edukacyjnych z zakresu cyberbezpieczeństwa w oparciu o normę ISO 27001 jest jej ukierunkowanie na funkcje procesowe obejmujące szeroki kontekst funkcjonowania organizacji. Norma wskazuje konieczność włączania we wszystkie zadania cyberbezpieczeństwa zarządzających i liderów, obejmuje cały łańcuch dostaw, przygotowanie planu, zabezpieczenie zasobów, realizację funkcji bezpieczeństwa i stworzenie stałych mechanizmów audytu.

Kolejnym kamieniem węgielnym dla programów edukacyjnych w zakresie edukacji specjalistów cyberbezpieczeństwa powinna być rama NIST33, zwłaszcza po jej zapowiadanej aktualizacji. Prócz tradycyjnie ważnych funkcji, jak Identyfikacja, Ochrona, Wykrywanie, Reagowanie i Przywracanie/Odbudowa, podkreśla ona rolę przygotowania całej organizacji i zarządzania procesami cyberbezpieczeństwa do głębokiej integracji z procesami firmy poprzez dodanie horyzontalnej funkcji Zarządzanie (Govern).

Dodatkowo rama NIST z jej branżowymi profilami odpowiada na potrzeby związane z wertykalizacją cyberbezpieczeństwa i pozwala na przygotowanie programów odnoszących się do specyfiki wybranych branż.

W związku z umieszczeniem odpowiedzialności za realizację funkcji zarządzania ryzykiem, zapewniania cyberbezpieczeństwa i ciągłości działania w regulacjach prawnych Unii Europejskiej i krajów członkowskich, bardzo istotnym wymogiem dla edukacji staje się programowe poszerzanie o te kwestie prawne. Takie akty legislacyjne jak NIS2, CRA (Cyber Resilience Akt) czy dyrektywa CER (Critical Entities Resilience) będą przez kolejne lata kształtowały wymagania formalne i organizacyjne w całym ekosystemie cyberbezpieczeństwa. Przegląd regulacji pozwoli również uwypuklić zagadnienia związane z obowiązkami firmy w zakresie współpracy z innymi podmiotami w krajowym i europejskim systemie bezpieczeństwa.

32) ISO/IEC 27001 – https://www.iso.org/standard/27001.
33) CYBERSECURITY FRAMEWORK – https://www.nist.gov/cyberframework.

Przegląd regulacji podkreśli również istotny trend poszerzania odpowiedzialności organizacji za cykl życia produktów i usług z komponentami cyfrowymi oraz konieczność brania pod uwagę cyberbezpieczeństwa łańcucha dostaw. Stworzy to podstawę pod włączenie w programy edukacyjne koncepcji *cybersecurity-by-design* i *cybersecurity-by-default*.

Wszystkie programy edukacyjne powinny zawierać odniesienia do ram kompetencji w zakresie cyberbezpieczeństwa.

Ramy umożliwiają wykorzystanie perspektywy procesowej, organizacyjnej i technicznej do poszerzenia katalogu kompetencji w zakresie cyberbezpieczeństwa potrzebnych dziś i w przyszłości. Ramy wskazują również inne uzupełniające kompetencje ważne z perspektywy biznesowej, w tym umiejętności komunikacji i współpracy. Ramy proponują też wspólny język opisu dziedziny cyberbezpieczeństwa i ułatwiają integrację pozyskanej wiedzy i umiejętności z praktyką zawodową.

Ze względu na sporą liczbę funkcjonujących w obszarze cyberbezpieczeństwa ram kwalifikacji – ich dobór do programu edukacyjnego jest kwestią indywidualną i zależną od profilu, zakresu i długości programu edukacyjnego.

REKOMENDACJE DLA STUDIÓW PODYPLOMOWYCH

Studia podyplomowe z zakresu cyberbezpieczeństwa, wśród osób gotowych inwestować w swoją karierę zawodową, cieszą się dużym zainteresowaniem. Pozwalają one zdobyć nowe umiejętności i wiedzę niezbędne do wykonywania określonego zawodu. Mogą również pomóc w zdobyciu certyfikatów lub uprawnień wymaganych w danej branży. Ukończenie takich studiów to zatem szansa na awans, podwyżkę lub zmianę pracy.

Z racji swojego szerokiego wymiaru czasowego (z reguły około 200 godzin wykładowych) i wymogu uprzedniego ukończenia studiów drugiego poziomu przez kandydatów, pozwalają na szersze potraktowanie zagadnień programowych.

W przypadku studiów poświęconych kompetencjom cyberbezpieczeństwa ich kluczowym aspektem jest sformułowanie celu studiów i określenie profilu docelowego absolwenta. Profil ten może być potraktowany wąsko i odnosić się do realizacji konkretnej roli zawodowej albo szeroko – przygotowując absolwenta do kilku ról związanych z przedmiotem studiów.

Niezależnie jednak od zakresu, w przypadku edukacji specjalistów cyberbezpieczeństwa istotne jest uwzględnienie w programie podstaw opisanych w poprzednim rozdziale, w tym ISO/EIC 27001, ramy NIST oraz zagadnień dotyczących głównych regulacji prawnych.

W zależności od profilu studiów warto się też zastanowić nad uwzględnieniem następujących rekomendacji:

Ukończenie studiów podyplomowych powinno umożliwić zrozumienie reguł całego ekosystemu cyberbezpieczeństwa. Z tego punktu widzenia istotne jest dodanie treści związanych z przeglądem strategii cyberbezpieczeństwa w Polsce i odniesienie polskiej strategii do zaleceń Unii Europejskiej oraz porównanie zakresu i podejścia polskiej strategii do strategii innych krajów, zwłaszcza tych, których strategie są wysoko oceniane. Wydaje się, że jednym z lepszych punktów odniesienia w obszarze strategii cyberbezpieczeństwa jest podejście Wielkiej Brytanii. Warto również przedstawić brytyjski sposób kształtowania świadomości roli i wymagań cyberbezpieczeństwa wśród zarządzających i właścicieli przedsiębiorstw.

Przy tworzeniu zestawu kompetencji absolwenta studiów warto uwzględnić ramę NICE[34] z racji jej szczegółowego charakteru i odniesienia do ramy NIST. Rama NICE definiuje również ponad 50 ról z zakresu cyberbezpieczeństwa, co może ułatwić absolwentom znalezienie interesującego ich profilu kompetencji.

W programie studiów podyplomowych warto też nawiązać do ramy SFIA[35] z racji jej dojrzałości, powiązania z obszarem ICT i precyzyjną definicją wymagań w obszarze uzupełniających kompetencji o charakterze społecznym, poznawczym i biznesowym.

Należy również przedstawić słuchaczkom i słuchaczom ramę ENISA European Cybersecurity Skills Framework[36], która jest prosta w użyciu i z definicji dobrze się wpisuje w organizację europejskiego systemu cyberbezpieczeństwa.

Dla zapewnienia praktycznego wymiaru studiów warto przedstawić ekosystem narzędzi uzupełniających, takich jak ramy NIST, NICE i SFIA.

Opisane powyżej zagadnienia nie stanowią oczywiście całego programu, ale ich uwzględnienie jest istotne z punktu widzenia budowy ogólnej struktury wiedzy i odniesienia do wymagań związanych z jej stosowaniem.

Należy się również zastanowić nad definicją wstępnych wymagań dla kandydatów na słuchaczy studiów podyplomowych. Potrzebna jest bowiem równowaga pomiędzy szerokim otwarciem uczelni dla wszystkich zainteresowanych, a postawieniem im pewnych oczekiwań.

W dyskusjach branżowych często słychać opinie, że techniczni specjaliści cyberbezpieczeństwa powinni mieć uprzednio zdobyte doświadczenie w działach IT związanych z utrzymaniem systemów i infrastruktury. Jednocześnie specjaliści zajmujący się kwestiami organizacyjnymi cyberbezpieczeństwa mogą odnieść korzyści, jeśli mają uprzednie doświadczenie z zarządzania organizacjami, połączone z doświadczeniem pracy w branżach mocno opartych o wykorzystanie technologii cyfrowych.

REKOMENDACJE DLA KURSÓW

W przypadku przygotowywania programów kursów dla specjalistów cyberbezpieczeństwa należy skupić się na realizacji celu związanego z uzyskaniem kompetencji potrzebnych do praktycznej realizacji wąsko zdefiniowanego zakresu działań. Dlatego przydatne jest spojrzenie na organizację kursu z perspektywy przygotowania jego uczestników do pracy w wybranej roli zawodowej.

W związku z tym należy odpowiednio zrównoważyć zakres edukacji ogólnej tworzącej podstawy pod wymogi planowanej przez uczestnika roli z konkretnymi kompetencjami praktycznymi, wymaganymi przy jej pełnieniu.

Z tej perspektywy dobrym punktem wyjścia do przygotowania kursów jest analiza takich ram kompetencji, jak European Cybersecurity Skills Framework lub UK Cyber Career Framework[37].

Dla kursów nastawionych na budowę ogólnych kompetencji szczególnie przydatne jest wykorzystanie podejścia prezentowanego w ramie brytyjskiej, która dobrze definiuje rolę Cyber Security Generalist. Obejmuje ona podstawy cyberbezpieczeństwa i podstawowe wymagania wobec kilku fundamentalnych ról. Takie podejście jest szczególnie przydatne dla kursów edukujących specjalistów cyberbezpieczeństwa dla małych i średnich organizacji, gdzie często sprawami cyberbezpieczeństwa zajmuje się jedna osoba lub bardzo mały zespół.

34) THE WORKFORCE FRAMEWORK FOR CYBERSECURITY – https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice.
35) SFIA VIEW: INFORMATION AND CYBER SECURITY – https://sfia-online.org/en/sfia-8/sfia-views/information-and-cyber-security?path=/glance.
36) EUROPEAN CYBERSECURITY SKILLS FRAMEWORK – https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.
37) CYBER SECURITY GENERALIST – https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/cyber-security-generalist/.

Warto też zastanowić się nad integracją kompetencji cyberbezpieczeństwa z podstawowymi kompetencjami IT z obszaru utrzymania systemów i infrastruktury informatycznej.

Jeśli kursy mają mieć bardziej specjalistyczny charakter, warto włączyć w ich zakres wymagania dla innych konkretnie zdefiniowanych ról w powyższych ramach (ECSF i UK CCF). Jako punkt odniesienia dla ogólnego zakresu wiedzy warto dla kursów wybrać ramę NIST, z racji jej powszechnego stosowania i wielu lat funkcjonowania na rynku.

Dodatkowo warto również skorzystać w edukacji w zakresie wymagań cyberbezpieczeństwa z opracowania ENISY. Jest to *Przewodnik po bezpieczeństwie cybernetycznym dla MŚP*[38], który został przetłumaczony na język polski albo z brytyjskiego Cyber Security Small Business Guide[39].

Dla podniesienia jakości programów kursów cyberbezpieczeństwa można też wykorzystać rekomendacje zawarte w *Poradniku cyberbezpieczeństwa dla doradców edukacyjnych i przedsiębiorców*, który jest istotnym uzupełnieniem niniejszego. Są w nim zawarte konkretne rekomendacje w sprawie przygotowania podstaw edukacji cyberbezpieczeństwa dla administratorów systemów oraz edukacji dla audytorów cyberbezpieczeństwa.

DEFINICJA RÓL ZAWODOWYCH W OBSZARZE CYBERBEZPIECZEŃSTWA

European Cybersecurity Skills Framework definiuje następujące role zawodowe w obszarze cyberbezpieczeństwa:

- CHIEF INFORMATION SECURITY OFFICER (CISO)
- CYBER INCIDENT RESPONDER
- CYBER LEGAL, POLICY & COMPLIANCE OFFICER
- CYBER THREAT INTELLIGENCE SPECIALIST
- CYBERSECURITY ARCHITECT
- CYBERSECURITY AUDITOR
- CYBERSECURITY EDUCATOR
- CYBERSECURITY IMPLEMENTER
- CYBERSECURITY RESEARCHER
- CYBERSECURITY RISK MANAGER
- DIGITAL FORENSICS INVESTIGATOR
- PENETRATION TESTER

Są one szczegółowo opisane w dokumencie, który można pobrać z witryny ENISA https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Z UK Cyber Career Framework warto przedstawić jako przykład opis odpowiedzialności, wymaganej wiedzy i umiejętności dla roli Cyber Security Generalist[40]:

CYBER SECURITY GENERALIST	
ZADANIA I ODPOWIEDZIALNOŚĆ	Cyber Security Generalist jest odpowiedzialny za każdy aspekt związany z bezpieczeństwem danych i systemów informacyjnych organizacji Do głównych jego zadań należą: • śledzenie podatności oprogramowania, systemów i sieci • rozpoznawanie i ocena zagrożeń cybernetycznych • rozpoznawanie i ocena ryzyka związanego z cyberbezpieczeństwem oraz rekomendowanie środków do zarządzania tym obszarem • projektowanie sposobów kontroli stanu bezpieczeństwa z uwzględnieniem obszaru rozwoju i tworzenia systemów informatycznych • tworzenie polityki i procedur z zakresu cyberbezpieczeństwa, zwłaszcza dotyczących bezpiecznej eksploatacji systemów • testowanie i raportowanie stanu bezpieczeństwa systemów i sieci organizacji • zarządzanie współpracą z dostawcami narzędzi i systemów bezpieczeństwa • wsparcie dla pracowników IT w zakresie ryzyka i wymagań związanych z cyberbezpieczeństwem • edukacja pracowników i zarządzających w zakresie ryzyka i wymagań związanych z cyberbezpieczeństwem, w tym procedur oraz bezpiecznych praktyk Dla osób z większym doświadczeniem warto również dodać: • odpowiedzialność za ogólną wydajność i bezpieczeństwo działających systemów • współpracę z kierownikami innych zespołów, aby zapewnić efektywne cyberbezpieczeństwo w całej organizacji • rekrutację, szkolenia i ocenę innych pracowników.

WIEDZA	Daje wiedzę pokrywającą następujące obszary:
	• Zarządzanie Ryzykiem i Zarządzanie Organizacją
	  • Systemy zarządzania bezpieczeństwem oraz organizacyjne kontrole bezpieczeństwa, w tym standardy, najlepsze praktyki i podejścia do oceny i redukcji ryzyka
	• Operacje Bezpieczeństwa i Zarządzanie Incydentami
	  • Konfiguracja, eksploatacja i utrzymanie bezpiecznych systemów, w tym wykrywanie i reagowanie na incydenty bezpieczeństwa oraz zbieranie i wykorzystywanie informacji o zagrożeniach
	Jeśli odpowiedzialności obejmują infrastrukturę przemysłową:
	• bezpieczeństwo systemów cyber-fizycznych
	• wyzwania związane z bezpieczeństwem systemów cyber-fizycznych, takich jak Internet Rzeczy oraz systemy przemysłowe, w tym modele ataków, dobre praktyki zapewniania bezpieczeństwa infrastruktury o dużych rozmiarach

38) Cybersecurity guide for SMEs – 12 steps to securing your business (28 czerwca 2021), ENISA, https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes [dostęp: 06.09.2023].
39) Cyber Security Small Business Guide (październik 2020), NCSC, https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf [dostęp: 06.09.2023].
40) CYBER SECURITY GENERALIST – https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/cyber-career-framework/cyber-security-generalist/ [dostęp: 06.09.2023].

DODATKOWA WIEDZA	• prawo i regulacje w zakresie cyberbezpieczeństwa • zagadnienia ochrony prywatności • zarządzanie dostępem • rodzaje ataków i malware • bezpieczeństwo sieci • bezpieczeństwo urządzeń dostępowych • zachowania użytkowników systemów informacyjnych • rozwój oprogramowania • kryminalistyka cyfrowa.
UMIEJĘTNOŚCI	Cechy osobowości: • samodyscyplina i samokontrola • efektywna komunikacja w sprawach technicznych • tworzenie raportów pisemnych i ustnych • zarządzanie dostawcami • priorytetyzacja skomplikowanych zestawów wymagań • rozumienie potrzeb biznesowych i użytkowników Umiejętności specjalistyczne (dodatkowo odniesione do ramy CIISec): • ocena i zarządzanie ryzykiem • zarządzanie projektami • zasady kontraktowania dostawców • szkolenia z zakresu świadomości cyberbezpieczeństwa • monitorowanie wydajności i bezpieczeństwa systemu • zarządzanie informacją
DODATKOWO PRZYDATNE DOŚWIADCZENIE	• IT helpdesk • zarządzanie projektami IT • zarządzanie systemami IT • zarządzanie operacjami biznesowymi

Poradnik cyberbezpieczeństwa dla doradców edukacyjnych i przedsiębiorców szczegółowo opisuje wymagania edukacji dwóch ról: specjalisty cyberbezpieczeństwa w zakresie administracji systemów oraz audytora cyberbezpieczeństwa. Ścieżki edukacyjne dla tych ról rekomendują umieszczenie w programach następujących zagadnień:

SPECJALISTA CYBERBEZPIECZEŃSTWA W ZAKRESIE ADMINISTRACJI SYSTEMÓW

Podstawy cyberbezpieczeństwa
- wprowadzenie do podstawowych pojęć i terminów związanych z cyberbezpieczeństwem
- znaczenie roli administratora w ochronie infrastruktury IT

Bezpieczeństwo systemów operacyjnych
- zasady bezpiecznej konfiguracji systemów operacyjnych (np. Windows, Linux)
- zarządzanie kontami i uprawnieniami użytkowników
- zabezpieczanie dostępu zdalnego do serwerów

Ochrona sieci
- bezpieczna konfiguracja urządzeń sieciowych, takich jak routery i firewalle
- monitorowanie ruchu sieciowego w celu wykrywania nieprawidłowości.
- zastosowanie zabezpieczeń przeciwko atakom typu DDoS

Zarządzanie incydentami i logami
- procedury reagowania na incydenty bezpieczeństwa
- analiza i monitorowanie logów w celu wykrywania podejrzanych aktywności
- prowadzenie audytów bezpieczeństwa

Zabezpieczanie aplikacji
- zapewnienie bezpieczeństwa aplikacji, takich jak serwery WWW i bazy danych.
- zarządzanie podatnościami aplikacji i ich łatanie
- wdrażanie zasad związanych z bezpiecznym programowaniem
- zabezpieczanie danych
- ochrona poufności danych i zarządzanie kluczami szyfrującymi
- zabezpieczenie danych w przechowywaniu i przesyłaniu
- planowanie i testowanie kopii zapasowych danych

Zabezpieczanie urządzeń mobilnych
- bezpieczeństwo urządzeń mobilnych używanych przez pracowników
- polityki BYOD (Bring Your Own Device) i zabezpieczenie danych firmowych

Pomocne techniczne certyfikaty branżowe
- CompTIA Security+
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)

A zalecenia dla programu przygotowania edukacji i audytorki i audytora cyberbezpieczeństwa wyglądają następująco:

AUDYTOR CYBERBEZPIECZEŃSTWA

Podstawy cyberbezpieczeństwa
- wprowadzenie do podstawowych pojęć i terminów związanych z cyberbezpieczeństwem
- zrozumienie podstawowych zagrożeń i wyzwań związanych z bezpieczeństwem informacji

Standardy i regulacje związane z cyberbezpieczeństwem
- zapoznanie się z międzynarodowymi standardami i regulacjami dotyczącymi cyberbezpieczeństwa, takimi jak ISO/IEC 27001, NIST Cybersecurity Framework, GDPR itp.

Procesy i procedury audytu
- zrozumienie procesów audytu i metodologii oceny ryzyka
- wykorzystanie narzędzi i technik audytorskich w kontekście cyberbezpieczeństwa

Audyt infrastruktury IT i architektury
- przeglądanie i ocena infrastruktury IT, w tym sieci, serwerów, urządzeń mobilnych i urządzeń końcowych
- ocena zabezpieczeń fizycznych i logicznych

Audyt aplikacji i systemów
- analiza i ocena zabezpieczeń aplikacji, w tym aplikacji internetowych i baz danych
- ocena bezpieczeństwa systemów operacyjnych i oprogramowania

Zarządzanie ryzykiem i planowanie ciągłości działania
- ocena procedur zarządzania ryzykiem organizacji
- planowanie i testowanie planów ciągłości działania w razie incydentu

Audyt zgodności i polityk bezpieczeństwa
- ocena zgodności organizacji z odpowiednimi standardami, regulacjami i politykami bezpieczeństwa
- weryfikacja czy polityki bezpieczeństwa są odpowiednio wdrożone i przestrzegane

Zarządzanie incydentami i reagowanie na naruszenia
- zapoznanie się z procedurami reagowania na incydenty bezpieczeństwa
- ocena, jak organizacja reaguje na wystąpienie naruszeń i próby włamań

Praktyczne ćwiczenia audytorskie
- praktyczne szkolenia i ćwiczenia audytorskie, które pozwalają praktykować umiejętności zdobyte podczas szkolenia

PODSUMOWANIE

Zaspokojenie potrzeb rynku pracy w zakresie liczby i jakości wykształcenia specjalistek i specjalistów cyberbezpieczeństwa pozostanie dużym wyzwaniem przez wiele kolejnych lat. Dlatego przygotowanie odpowiednich programów edukacyjnych ukierunkowanych na cyberbezpieczeństwo jest jednym z kluczowych zadań branży.

Przedstawione rekomendacje, analiza i przykładowy poradnik tworzące *Kompendium Cyberbezpieczeństwa* mogą stanowić dobry punkt wyjścia do przygotowania odpowiednich programów edukacyjnych i dyskusji na temat ich struktury.

Ważne jest, aby dla zapewnienia jakości programów edukacyjnych i skrócenia czasu ich przygotowania oprzeć je o standardy używane w całej branży cyberbezpieczeństwa, jak sugeruje autor artykułu zawartego w publikacji Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo *Międzynarodowe narzędzia opisu kompetencji cyberbezpieczeństwa – nie wymyślajmy koła od nowa*[41].

41) Artykuł w Kompetencje, edukacja i rynek pracy w sektorze telekomunikacja i cyberbezpieczeństwo – dziś i jutro, Sektorowa Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Warszawa 2021 – https://srtcb.radasektorowa.pl/images/raporty/Kompetencje_edukacja_i_rynek_pracy_w_sektorze_telekomunikacja.pdf [dostęp: 06.09.2023].

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

SEKTOROWA RADA DS. KOMPETENCJI TELEKOMUNIKACJA I CYBERBEZPIECZEŃSTWO

Rada inicjuje i uczestniczy w przedsięwzięciach związanych z potrzebami kompetencyjnymi w obszarach telekomunikacji i cyberbezpieczeństwa, pomagając dostosować ofertę edukacyjną do wymagań rynku pracy w tym sektorze.

Rada pomaga dostosowywać ofertę edukacyjną do obecnych wymagań rynku pracy w sektorach telekomunikacji i cyberbezpieczeństwa m.in. poprzez:

- rekomendowanie rozwiązań /zmian legislacyjnych w edukacji i jej dostosowania do potrzeb rynku pracy w sektorze
- wskazywanie obszarów badawczych dotyczących kompetencji w sektorach oraz zlecanie tego rodzaju badań
- identyfikację potrzeb w zakresie aktualizacji Sektorowej Ramy Kwalifikacji oraz definiowanie poszczególnych kwalifikacji
- przekazywanie informacji nt. zapotrzebowania na kompetencje pracowników do instytucji edukacyjnych i rynku pracy, aby wpłynąć na poprawę ich skuteczności
- obsługę działania 2.21 typ 4 POWER (szkolenia lub doradztwo wynikające z rekomendacji Sektorowych Rad ds. Kompetencji), w szczególności opracowanie oraz aktualizacja rekomendacji dotyczących zapotrzebowania na kompetencje w sektorze.

Rada wydała dotychczas dwie rekomendacje rozwojowe – nadzwyczajną, tzw. antycovidową, oraz zwyczajną. Ich celem było wskazanie najpilniejszych potrzeb kompetencyjnych w sektorze telekomunikacji i cyberbezpieczeństwa.

Działając na styku edukacji z biznesem, Rada współorganizuje coroczne Forum Współpracy Edukacji i Biznesu EDUMIXER. Jego celem jest wypracowanie propozycji zmian w programach kształcenia przyszłych pracobiorców, które będą uwzględniały rozwój technologiczny oraz potrzeby rynku pracy.

e-mail: rada.telekomunikacja@pti.org.pl

www.srtcb.radasektorowa.pl

Projekt „Utworzenie i funkcjonowanie Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo" jest realizowany w ramach Osi priorytetowej II: Efektywne polityki publiczne dla rynku pracy, gospodarki i edukacji oraz Działania 2.12 Zwiększenie wiedzy o potrzebach kwalifikacyjno-zawodowych w poszczególnych sektorach gospodarki.

Projekt nr UDA-POWR.02.12.00- 00-SR03/18 jest współfinansowany z Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020.

PARP
Grupa PFR

Sektorowa Rada
ds. Kompetencji
Telekomunikacja
i Cyberbezpieczeństwo

www.srtcb.radasektorowa.pl

Partnerzy projektu:

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

PIIT

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

Warszawa, wrzesień 2023