Zeszyty Naukowe
Wyższej Szkoły Ekonomii i Informatyki
Nr 20/2024, s. 133-160
DOI: XXXXXX

ISSN 1734-5391
e-ISSN 2957-2223

Zbigniew Handzel
dr inż., prof. WSEI, Zakład Informatyki
Wyższa Szkoła Ekonomii i Informatyki
w Krakowie (WSEI)
email: zhandzel@wsei.edu.pl
ORCID: 0000-0003-1470-6592

Netbloger
Wyższa Szkoła Ekonomii i Informatyki
w Krakowie, Zakład Informatyki

Anna Stolińska
dr, prof. WSEI, Zakład Informatyki
Wyższa Szkoła Ekonomii i Informatyki
w Krakowie (WSEI)
email: astolinska@wsei.edu.pl
ORCID: 0000-0003-0979-011X

Krzysztof Tyl
dr inż., IT Challenge,
University of Vienna,
Austria

Wojciech Urbanczyk
dr inż., Faculty of Computer Science,
University of Vienna,
Austria

Jan Werewka
dr hab. inż., prof. WSEI, Zakład Informatyki
Wyższa Szkoła Ekonomii i Informatyki
w Krakowie (WSEI)
email: jwerewka@wsei.edu.pl
ORCID: 0000-0002-2308-2374

STUDIA W ZAKRESIE CYBERBEZPIECZEŃSTWA, A ZAPEWNIENIE POTRZEB BEZPIECZEŃSTWA IT/OT W PRZEDSIĘBIORSTWACH

CYBERSECURITY STUDIES AND ENSURING IT/OT SECURITY NEEDS IN ENTERPRISES

Słowa kluczowe: *cyberbezpieczeństwo, programy studiów, bezpieczeństwo cyfrowe firm*
Key words: *cybersecurity, study programs, digital security of companies*

JEL Classification: A2, C8, I2, L2, P4

Streszczenie

W dobie rosnącej cyfryzacji przedsiębiorstw kwestia cyberbezpieczeństwa staje się jednym z kluczowych wyzwań współczesnej gospodarki. W obliczu coraz bardziej zaawansowanych ataków cybernetycznych, przedsiębiorstwa na całym świecie muszą nie tylko wdrażać nowe technologie, ale również inwestować w pracowników. W zależności od struktury firmy

stosowane są różne podejścia zatrudniania specjalistów, którzy mają zapewnić bezpieczeństwo cyfrowe w przedsiębiorstwie. Dokonywane jest to przez zatrudnianie specjalistów w zakresie cyberbezpieczeństwa, zawieranie umów ze specjalistycznymi firmami lub działania doraźne, takie jak zlecanie firmom przeprowadzenie audytu i wdrożenie rozwiązań bezpieczeństwa cyfrowego. Z drugiej strony dla uczelni ważne jest przygotowanie studentów do pracy związanej z cyberbezpieczeństwem firm. Celem niniejszego artykułu jest przedstawienie propozycji budowania kompetencji wg zasady stosowanej w metodykach zwinnych zarządzania (generalist, specialist), zgodnie z którą członkowie zespołu powinni być specjalistami w jednym obszarze, a w pozostałych powinni mieć kompetencje na poziomie ogólnym. Taka koncepcja budowania kompetencji wynika z faktu, że uczelnie nie są w stanie w pełni sprostać wymaganiom wobec kompetencji studentów, stawianym przez firmy. Dodatkowo, artykuł analizuje współczesne wyzwania bezpieczeństwa związane z integracją systemów IT i OT w przedsiębiorstwach. Ważnymi zagadnieniami tych systemów są sprzeczne ze sobą rozwiązania integracji i segmentacji (izolacji) elementów systemów, mające swoje korzyści i wady ze względu na cyberbezpieczeństwo. W zrozumieniu potrzeb i luk kompetencyjnych określających potrzeby szkoleniowe dla zatrudnianych absolwentów pomoże podejście holistyczne, wsparte poprzez modele architektury korporacyjnej.

Abstract

In the era of increasing digitalization of enterprises, the issue of cybersecurity is becoming one of the key challenges of the modern economy. In the face of increasingly sophisticated cyberattacks, companies worldwide must not only implement new technologies but also invest in their employees. Depending on the structure of the company, various approaches are used to hire specialists responsible for ensuring digital security within the organization. This is achieved by hiring cybersecurity specialists, entering into agreements with specialized firms, or taking ad-hoc actions such as commissioning companies to conduct audits and implement digital security solutions. On the other hand, it is crucial for universities to prepare students for work related to corporate cybersecurity. The purpose of this article is to propose a method for building competencies based on the principle applied in agile management methodologies (generalist, specialist), according to which team members should be specialists in one area and have general-level competencies in others. This concept of competency building stems from the fact that universities are unable to fully meet the

competency requirements set by companies for their students. Additionally, the article analyzes contemporary security challenges related to the integration of IT and OT systems in enterprises. Key issues in these systems involve conflicting solutions of integration and segmentation (isolation) of system components, which have both advantages and disadvantages in terms of cybersecurity. Understanding the needs and competency gaps that define training requirements for newly hired graduates can be facilitated by a holistic approach supported by enterprise architecture models.

WSTĘP

Aktualnie w firmach pierwszorzędne znaczenie ma zapewnienie bezpieczeństwa cyfrowego. Jednym ze sposobów radzenia sobie z tego rodzaju problemem jest zatrudnienie specjalistów z zakresu bezpieczeństwa cyfrowego. W zależności od potrzeb specjaliści ci mogą być zatrudniani na różnych stanowiskach, tj.: specjalista ds. cyberbezpieczeństwa, analityk bezpieczeństwa informatycznego, administrator systemów bezpieczeństwa, audytor bezpieczeństwa IT, konsultant ds. zarządzania ryzykiem i zabezpieczeń, specjalista ds. reagowania na incydenty cybernetyczne, penetrator testujący bezpieczeństwo, specjalista ds. ochrony danych osobowych i zgodności z przepisami, inżynier bezpieczeństwa sieciowego. Lista tych specjalistów jest długa i wskazuje na potrzeby posiadania kompetencji zgodnie z proponowanym stanowiskiem.

Dodatkowym problemem jest to, że przy rozpatrywaniu bezpieczeństwa bardzo często rozważa się bezpieczeństwo IT w oderwaniu od działalności operacyjnej przedsiębiorstwa. Okazuje się, że w wielu przypadkach bezpieczeństwo operacyjne odgrywa kluczową rolę. Bezpieczeństwo IT rozumiane jest jako bezpieczeństwo, w którym dane są najważniejszym aktywem, których bezpieczeństwo powinno być brane pod uwagę w pierwszej kolejności. Dla wielu firm jednakże zakłócenie działalności operacyjnej może przynieść wielkie szkody. Przez lata istniała tendencja ścisłej integracji działalności IT (Information Technology) i OT (Operational Technology). Miało to wiele zalet, a w szczególności to, iż z jednego stanowiska mogliśmy kontrolować i sterować działalnością operacyjną. Taki sposób integracji niósł duże ryzyko tego, że poprzez systemy IT można było zakłócić działalność operacyjną. Rozwiązania tego problemu szukano w segmentacji systemów IT/OT. W tym przypadku przekazywanie danych pomiędzy segmentami było odpowiednio kontrolowane.

Zwykle programy studiów dotyczących technologii IT koncentrują się w dużej mierze na bezpieczeństwie tych technologii. Jednakże wraz ze wzrostem złożoności architektury IT w przedsiębiorstwach o charakterze produkcyjnym bardzo ważne stało się uwzględnienie bezpieczeństwa na poziomie operacyjnym w powiązaniu z bezpieczeństwem IT. Tradycyjnie w przedsiębiorstwie posiadającym rożnego rodzaju formy produkcji wyróżniamy dwa obszary IT (Information Technolgy) i OT (Operation Technology), dla których stosuje się różne podejścia. Zazwyczaj OT dotyczy bezpiecznych operacji i sterowania fizycznymi urządzeniami i procesami, natomiast IT dotyczy zarządzania informacją i komunikacją oraz przetwarzania danych i informacji. We współczesnym świecie następuje konwergencja obu obszarów, co może powodować zagrożenie bezpieczeństwa całego przedsiębiorstwa w przypadku łatwego dostania się z jednego obszaru do drugiego. Dlatego dla wielu systemów IT/OT ważne jest połączenie zagadnień bezpieczeństwa dla obu tych obszarów. Poniższe wybrane przykłady pokazują, że bezpieczeństwo systemów OT jest równie ważne jak bezpieczeństwo systemów IT [1]:

1. Atak na rurociąg przesyłowy ropy naftowej. W 2021 (Colonial Pipeline) spowodował zawieszenie operacji przesyłania ropy. Hakerzy uzyskali dostęp do systemu poprzez użycie konta do wirtualnej, prywatnej sieci.
2. Atak na niemiecką stalownię. W 2014 roku niemiecka stalownia została zaatakowana przez hakerów, co spowodowało przerwanie pracy pieca hutniczego. Atakujący uzyskali dostęp do sieci biznesowej, a następnie do sieci SCADA/ICS (Supervisory Control and Data Acquisition / Industrial Control Systems).
3. Awaria systemu kontroli lotów. W 2019 roku awaria systemu kontroli lotów w Stanach Zjednoczonych spowodowała zakłócenia w ruchu lotniczym w wielu częściach kraju. Incydent ten wywołał obawy dotyczące bezpieczeństwa systemów krytycznych i potrzeby zapewnienia odpowiedniego poziomu ochrony przed awariami.

Pod względem bezpieczeństwa połączonych systemów IT i OT należy uwzględnić sprawdzone i istniejące już na rynku standardy bezpieczeństwa. Różnice technologiczne pomiędzy IT i OT, które tradycyjnie oddzielały te różne dyscypliny, obecnie szybko zanikają. Aby zapewnić odpowiedni poziom bezpieczeństwa, nie wystarczy już polegać na specyfice technologii stosowanych w infrastrukturze przemysłowej.

Jednym z celów tego artykułu jest analiza luk kompetencyjnych absolwentów w szczególności dotyczących systemów IT/OT, którzy będą

zatrudnieni w firmach jako specjaliści w zakresie cyberbezpieczeństwa. Znajomość tych luk jest bardzo istotna, gdyż incydenty cyberbezpieczeństwa są zjawiskami losowymi, obciążonymi różnymi ryzykami. Ponieważ absolwenci nie mogą być specjalistami w każdej dziedzinie, to rozważa się tutaj rozwijanie kompetencji zgodnie z literą T. Oznacza to, że absolwent powinien mieć wiedzę ogólną z wielu obszarów bezpieczeństwa (ang. generalist), natomiast w jednym z nich powinien być specjalistą. Wiedza ogólna jest tu istotna, gdyż pracownik powinien być świadomy różnych zagrożeń i konieczności zwracania się o pomoc do innych specjalistów. Do zdobywania wiedzy ogólnej mogą posłużyć rozwiązania architektury korporacyjnej, które cechują się podejściem całościowym (holistycznym). Chcemy przy tym podkreślić znaczenie współpracy między uczelniami, a przemysłem w celu lepszego przygotowania studentów do realiów pracy w sektorze cyberbezpieczeństwa.

ROZWÓJ KOMPETENCJI BEZPIECZEŃSTWA CYFROWEGO PRZEDSIĘBIORSTW NA STUDIACH INFORMATYCZNYCH

W niniejszym artykule poddano analizie studia na kierunku informatyka stosowana, na których wyodrębniono specjalizacje przedstawione jako moduły. Zakłada się w nich, że absolwent specjalności cyfrowego bezpieczeństwa przedsiębiorstw będzie zdolny do rozwiązywania złożonych problemów związanych z bezpieczeństwem informacji i systemów informatycznych. Będzie posiadał wiedzę i umiejętności niezbędne do analizy, zapobiegania i reagowania na zagrożenia cybernetyczne oraz ochrony przedsiębiorstw w cyberprzestrzeni. Absolwent specjalności „Cyberbezpieczeństwo przedsiębiorstw" studiów II stopnia może pracować na różnych stanowiskach w obszarze cyberbezpieczeństwa w przedsiębiorstwach, instytucjach państwowych, kancelariach audytorskich, firmach konsultingowych, agencjach bezpieczeństwa informacji oraz w działach IT. Na rozpatrywanym kierunku Informatyki stosowanej wydzielono przedmiot kierunkowy Cyberbezpieczeństwo przedsiębiorstw (4 ECTS), którego nazwa jest jednakowa jak wspomniany powyżej moduł specjalnościowy. Na tym module prowadzone są następujące przedmioty (każdy za 4 ECTS):

1. Standardy cyberbezpieczeństwa.
2. CCNA CyberOps Associate.
3. CCNP Enterprise.

4. DevNet Associate.
5. Laboratorium cyberbezpieczeństwa.

Przedstawione rozwiązanie zakłada, że student uzyska pogłębioną wiedzę specjalistyczną z zakresu bezpieczeństwa cyfrowego bazując na rozwiązaniach CISCO. Natomiast w ramach innych przedmiotów powinien uzyskać ogólną wiedzę. Wiedza szczegółowa powinna pozwolić na wykonanie wielu zadań technicznych takich jak: konfigurowanie narzędzi monitorujących i wykrywanie zagrożeń, zarządzanie incydentami bezpieczeństwa oraz przeprowadzanie analizy działań reaktywnych i proaktywnych; testowanie i analiza bezpieczeństwa: przeprowadzanie testów bezpieczeństwa aplikacji i infrastruktury, analizowanie logów i zdarzeń oraz wykrywanie i reagowanie na incydenty.

Kompetencje ogólne absolwenta będą obejmować m.in.:

- Projektowanie i implementację rozwiązań bezpieczeństwa, które polega na identyfikowaniu i analizie zagrożeń oraz tworzenie strategii i rozwiązań mających na celu zabezpieczenie systemów informatycznych przedsiębiorstw.
- Zarządzanie ryzykiem i przeprowadzenie audytów bezpieczeństwa polegających na ocenie ryzyka związanego z cyberbezpieczeństwem przedsiębiorstw, stosowaniu metodyki zarządzania bezpieczeństwem oraz przeprowadzanie audytów bezpieczeństwa. Przewidziana jest także identyfikacja słabych punktów w systemach informatycznych i opracowanie zabezpieczeń.
- Opracowywanie strategii reagowania na zagrożenia i doskonalenie procesów bezpieczeństwa. W wyniku tego wprowadzane są zmiany organizacyjne i rozwijana jest kultura bezpieczeństwa w przedsiębiorstwach.

Tak zbudowany moduł ma tę zaletę, że punkt ciężkości kompetencji bazuje na kursach i certyfikatach CISCO. Ten wybór ma swoje uzasadnienie w tym, że rozwiązania wspomnianej firmy są bardzo rozpowszechnione w przedsiębiorstwach.

Na rynku technologii informatycznych oprócz Cisco Systems pojawiły się w ostatnich latach konkurencyjne produkty takich firm jak: Fortinet, CrowdStrike, Netscaler, Amazon AWS, Microsoft Azure, PaloAlto, Juniper, czy Armis. Większość produktów tych firm konkuruje lepiej lub gorzej ze standardami wyznaczanymi od wielu już lat przez technologie Cisco. Dotyczą one rozwiązań w zakresie cyberbezpieczeństwa takich jak: Zero Trust, obrona przed np. Ransomware, czy spełniania wymogów standardów ISO 27001, ISO 42001 oraz BSI. Przyszłość IT należy do świata

wielu dostawców. Tylko ktoś, kto jest nieświadomy rozwoju IT, decyduje się na korzystanie z jednego dostawcy we wszystkich kwestiach związanych z technologiami teleinformatycznymi. Warto jednakże podkreślić, iż wspomniane technologie są oparte na standardach i protokołach, zatem dokładne zapoznanie się z jedną z tych platform i ugruntowanie wiedzy na temat jej wykorzystania powinno bez problemu pozwolić absolwentowi omawianej specjalności na łatwe nauczenie się korzystania z pozostałych rozwiązań.

Jednym z powodów wyboru w omawianym programie studiów rozwiązań Cisco jest to, iż największym problemem konkurencyjnych rozwiązań jest brak wykwalifikowanych kandydatów na stanowiska inżynierów, czy administratorów sieci IT. Autorzy niniejszego artykułu, będący jednocześnie twórcami programu studiów na kierunku Informatyka stosowana są świadomi tego, iż Cisco nie jest najtańszym z rozwiązań, ale argumentem przemawiającym za tym wyborem jest to, iż certyfikaty CCNA i CCNP są najbardziej powszechne i można się z nimi spotkać w wielu uniwersytetach i innych szkołach wyższych. Kursy dotyczące innych niż Cisco rozwiązań niestety w przypadku uczelni są rzadkością. Ponadto autorzy niniejszego artykułu pragną podkreślić, iż w przypadku firm chcących korzystać z rozwiązań innych dostawców niż Cisco, tj. np. produkty firm Fortinet lub PaloAlto, prawdopodobnie będą one musiały zatrudnić kandydatów posiadających już certyfikat CCNA lub CCNP i zainwestować w ich dalsze szkolenie i rozwój.

Produkty Cisco są popularne i dobrze znane, a ponadto istnieją na rynku od długiego już czasu, a jednocześnie Cisco ustanowiło wysoko poprzeczkę w zakresie szkoleń i certyfikatów. CCNA nadal jest de facto ścieżką dostępu do certyfikatu sieciowego, od której większość specjalistów zaczyna swoją karierę. Chociaż certyfikaty Cisco, które można uzyskać następnie po CCNA są bardzo skoncentrowane na produktach Cisco i nie są ogólnymi certyfikatami sieciowymi, to powinno się na to patrzeć jak na naturalną ciągłość biznesową.

Ponadto warto w tym miejscu podkreślić, że kiedy dobrze pozna się środowisko Cisco, można łatwo poznać większość środowisk innych dostawców. Trzeba tylko „dostosować" pewne pojęcia i słownictwo innego typu sprzętów, co dla specjalistów nie powinno być zbyt skomplikowane. Certyfikat CCNA trzeba w tym przypadku potraktować jako podstawę wiedzy ogólnej i z pewnością nie zaszkodzi dowiedzieć się jak działa np. IOS. Podsumowując, powinno się doceniać kwalifikacje uzyskane podczas pracy z systemami Cisco, ponieważ dają one solidne podstawy wiedzy

niezbędnej do pracy z produktami innych dostawców. Znalezienie specjalistów posiadających certyfikaty i doświadczenie np. PaloAlto i jednocześnie wiedzę ogólną z sieci IT będzie trudne. W tym przypadku będzie się wybierać pomiędzy dopłatą za sprzęt Cisco, albo dopłatą dla inżyniera ze znajomością technologii PaloAlto czy Fortinet. W ten sposób można próbować oszacować koszt związany z luką kompetencyjną.

Omawiany moduł Cyberbezpieczeństwa przedsiębiorstw zapewnia studentom zdobycie wiedzy nie tylko z zakresu technicznych aspektów bezpieczeństwa, ale również z dziedzin takich jak prawo, zarządzanie ryzykiem oraz ekonomia. Pozwala to na przygotowanie przyszłych specjalistów, którzy będą w stanie holistycznie podchodzić do problemów związanych z bezpieczeństwem cyfrowym w przedsiębiorstwach, uwzględniając nie tylko aspekty techniczne, ale również organizacyjne i prawne.

STUDIA BAZUJĄCE NA KURSACH I CERTYFIKATACH Z ZAKRESU BEZPIECZEŃSTWA CYFROWEGO PRZEDSIĘBIORSTW

W praktyce firmowej i uczelnianej rozpowszechniły się kursy i certyfikaty związane z bezpieczeństwem IT. Kursy te zwykle są dobrze dostosowane do potrzeb różnorodnych firm. Takie certyfikaty potwierdzają wiedzę oraz rozwijają szereg umiejętności w zakresie bezpieczeństwa cyfrowego. Na wielu z tych kursów przekazuje się informacje ogólne z zakresu podstaw bezpieczeństwa cyfrowego przedsiębiorstw oraz omawia podstawowe standardy cyberbezpieczeństwa. Zwykle w tym przypadku jest dostarczana wiedza uniwersalna i niezależna od dostawców oprogramowania i sprzętu komputerowego. Inną grupą są kursy i certyfikaty rozwijane przez instytucje i firmy dostarczające rozwiązania z zakresu bezpieczeństwa. Kursy i certyfikaty CISCO, które zyskały na popularności to przykładowo:

1. CCNA CyberOps Associate [2]. Certyfikat przeznaczony dla specjalistów zajmujących się wykrywaniem i reagowaniem na incydenty cybernetyczne.
2. CCNP Enterprise (Cisco Certified Network Professional – Enterprise) [3]). Zaawansowany certyfikat Cisco, który skupia się na zaawansowanych umiejętnościach z zakresu sieci komputerowych i infrastruktury przedsiębiorstwa. Dotyczy rozwoju umiejętności takich jak: routing, przełączanie, bezpieczeństwo, rozwiązywa-

nie problemów i zarządzanie infrastrukturą sieciową w dużych organizacjach.

3. DevNet Associate (Cisco Certified DevNet Associate) [4]). Jest to certyfikat odpowiedni zarówno dla programistów, jak i administratorów sieci, którzy chcą nauczyć się programować i automatyzować operacje sieciowe przy użyciu narzędzi i technologii Cisco. Certyfikat dotyczy podstaw programowania, zarządzania infrastrukturą sieciową w sposób programowy, rozwiązywania problemów i tworzenia aplikacji zorientowanych na rozwiązania sieciowe.

Cyberbezpieczeństwo za główny cel stawia chronienie zasobów przedsiębiorstwa. Przyglądając się rynkowi oraz przedsiębiorstwom możemy wyodrębnić następujące czynniki, które mają wpływ na zasoby chronione w przedsiębiorstwie:

- miejsce składowania/przetwarzania/transmisji danych: w siedzibie firmy (On premise), w chmurze (Cloud),
- platformy składowania/przetwarzania/transmisji danych: monoblok, mikroserwisy,
- technologia użyta do składowania/przetwarzania/transmisji danych: tradycyjne podejście do technologii tzw legacy (odziedziczone), programowe podejście do technologii tzw. Software Defined (zdefiniowane programowo).

Powyższe czynniki pokazują pewien trend do spajania wielu odrębnych dyscyplin, technologii w jedną całość powodując komplikacje w procesie np. bezpiecznego utrzymania platformy/produktu, a co za tym idzie bezpieczeństwa samych danych, które produkt generuje. Można także zaobserwować w przedsiębiorstwach kierunek zmierzający do minimalizacji czasu przestoju w dostępie do danych, co czasami wiąże się z migracją do chmury obliczeniowej.

Wszystkie wymienione zagadnienia oznaczają, że technologie używane na przestrzeni ostatnich kilkunastu lat są coraz bardziej skomplikowane i złożone. Sytuacja ta oczywiście wpływa niekorzystnie z punktu widzenia przedsiębiorstwa oraz wyspecjalizowanego działu odpowiedzialnego za utrzymanie „produktu", a przede wszystkim ma ogromny wpływ na sam proces utrzymania „bezpiecznej platformy", czy bezpieczeństwa danych, które ten produkt generuje oraz przechowuje.

Biorąc pod uwagę powyżej wymienione argumenty możemy jednoznacznie stwierdzić, że nie ma jednej ścieżki kształcenia, kursu, który w/w pojęcia zawarłby w całości. W tej sytuacji byliśmy zmuszeni jako uczelnia do szukania „złotego środka", czyli podejścia interdyscyplinarnego w za-

kresie zagadnień, które mogłyby pokryć oczekiwania rynku oraz kształcić adekwatnie do zapotrzebowania studentów z cyberbezpieczeństwa.

Drugim niezmiernie ważnym elementem podczas wyboru kursów, na których oparliśmy kluczowe przedmioty w procesie kształcenia było to, aby kursy były „utrzymywane" przez duże jednostki z branży, które posiadają wieloletnie doświadczenie w danej dziedzinie. Stąd wybór padł na kursy firmy Cisco, dające gwarancję, że zagadnienia zawarte w kursach będą aktualne oraz będą na bieżąco aktualizowane.

Aktualny program kształcenia na kierunku studiów z zakresu cyberbezpieczeństwa bazuje na trzech filarach, które swoim zakresem obejmują trzy główne elementy z cyberbezpieczeństwa i jak również pokrywają się z trzema zespołami, które możemy spotykać w przedsiębiorstwach. Są to zespoły odpowiedzialne za:

- bezpieczeństwo systemów – SecOps,
- bezpieczeństwo sieci – SecNet,
- programowanie sieci i systemów – DevNet/DevOps.

Na takim założeniu bazowaliśmy określając listę szkoleń, które są w stanie sprostać naszym wymaganiom oraz zapotrzebowaniem rynku co do przyszłych pracowników w przedsiębiorstwie. Wybór padł na następujące kursy:

a) CCNP Enterprise – 350-401 ENCOR

Kurs ten jest najczęściej wybieranym kursem CISCO na poziomie profesjonalnym. Kurs ten obejmuje tematy: architektura, wirtualizacja, infrastruktura, diagnostyka, bezpieczeństwo, automatyzacja [5]. Rozpatrywany kurs w najnowszej wersji 8 stanowi punkt wyjścia do dalszego rozwoju i określenia kierunku, w którym chcemy poszerzyć swoje możliwości. Jest kilka ścieżek poszerzających wiedzę z tego zakresu:

- zaawansowane technologie rutowania i przełączania 300-410 ENARSI,
- technologie związane z rozległymi sieciami programowalnymi tzw. SD-WAN 300-415 ENSDWI,
- projektowanie sieci typu Campus, WAN oraz SDA 300-420 ENSLD
- technologie sieci bezprzewodowych oraz mobilnych WLAN 300-425 ENWLSD,
- technologie sieci multikastowych, QoS, bezpieczeństwo i hardening urządzeń 300-430 ENWLSI,
- automatyzacja sieci, programowanie, API oraz narzędzia 300-435 ENAUTO.

Ścieżki te dają duże możliwości dalszej edukacji pod kątem specjalizacji z danej dyscypliny adekwatnie do zapotrzebowania w przedsiębiorstwie.

Kurs CCNP Enterprise stał się bazą do opracowania przedmiotu o tej samej nazwie jako jeden z filarów do zajęć dydaktycznych prowadzonych w formie konwersatoriów oraz praktycznych laboratoriów. Po ukończeniu tego przedmiotu oraz spełnieniu określonych warunków student jest uprawniony do otrzymania certyfikatu CISCO ukończenia kursu, oraz uzyskuje zniżki na egzamin zewnętrzny.

b) CyberOps Associate 200-201 CBROPS

Kurs CyberOps został opracowany przez firmę CISCO dla osób o profilu Security Operations Center. Kurs ten zastąpił starszy kurs oferowany przez firmę CISCO o nazwie CCNA CyberOps. Kurs ten jest najczęściej wybieranym kursem CISCO na poziomie podstawowym obejmującym zagadnienia budowy, monitorowania bezpiecznych sieci oraz systemów komputerowych przy użyciu specjalizowanych narzędzi oraz technologii CISCO. Poruszane tematy dotyczą bezpieczeństwa danych, systemów oraz sieci: projektowanie, budowanie, monitorowanie, reagowanie, automatyzacja [6]. Kurs ten stanowi punkt wyjścia do dalszego rozwoju kompetencji:

- cyberbezpieczeństwo na poziomie zaawansowanym 350-201 CBRCOR,
- analiza kryminalistyczna oraz incydenty 300-215 CBRFIR,
- zagrożenia w systemach oraz sieciach 300-220 CBRTHD.

Kurs ten stał się bazą do opracowania przedmiotu o tej samej nazwie prowadzonego w formie konwersatoriów oraz praktycznych laboratoriów. Po ukończeniu tego przedmiotu oraz spełnieniu określonych warunków student jest uprawniony do uzyskania certyfikatu CISCO po ukończenia kursu oraz uzyskuje zniżki na egzamin zewnętrzny.

c) DevNet Associate 200-901 DEVASC

Kurs DevNet Associate (DEVASC) został opracowany przez firmę CISCO zarówno dla programistów, jak i administratorów sieci, którzy chcą nauczyć się programować i automatyzować sieci przy użyciu narzędzi i technologii Cisco. Kurs ten jest pierwszym kursem CISCO na poziomie podstawowym obejmującym zagadnienia związane z: programowaniem z wykorzystaniem języka Python, zarządzaniem urządzeniami sieciowymi za pomocą interfejsu API, podstawowymi zagadnieniami związanymi z sieciami, automatyzacje zadań sieciowych, IaC oraz DevOps przy użyciu języka Python [4]. Pełna lista zagadnień poruszanych dla każdej w/w pozycji znajduje się pod linkiem [7]. Kurs ten stanowi punkt wyjścia do dalszego rozwoju kompetencji w zakresie programowania sieci. Przykładowe możliwe dalsze ścieżki rozwoju:

- Cisco Certified DevNet Professional
- Cisco Certified DevNet Expert

Kurs ten stał się bazą do opracowania przedmiotu o tej samej nazwie, jako kolejny z filarów dla zajęć dydaktycznych prowadzonych w formie konwersatoriów oraz praktycznych laboratoriów. Po ukończeniu tego przedmiotu oraz spełnieniu określonych warunków student jest uprawniony do uzyskania certyfikatu CISCO po ukończenia kursu oraz uzyskuje zniżki na egzamin zewnętrzny.

Dzięki zintegrowaniu kluczowych kursów i certyfikacji CISCO, przedstawiony powyżej program kształcenia skoncentrował się na dostarczeniu specjalistycznej wiedzy, która jest zgodna z obecnymi wymaganiami rynku. Absolwenci będą dobrze przygotowani do pracy w dynamicznym i wymagającym środowisku, gdzie będą mogli skutecznie odpowiadać na zagrożenia cybernetyczne, projektować i implementować strategie bezpieczeństwa, a także zarządzać ryzykiem w różnorodnych kontekstach przedsiębiorstw. Ich kompetencje będą solidnie osadzone w głównych nurtach potrzeb współczesnych firm, co, w założeniach twórców programu, uczyni ich cenionymi specjalistami na rynku pracy, gotowymi do podjęcia wyzwań w obszarze cyberbezpieczeństwa. Należy jednak zauważyć, że współczesne przedsiębiorstwa coraz częściej stają przed wyzwaniem zapewnienia bezpieczeństwa złożonych systemów, które integrują technologie IT (Information Technology) z OT (Operational Technology). Konwergencja tych dwóch obszarów, choć przynosi liczne korzyści, generuje również nowe zagrożenia, które wymagają unikalnych kompetencji od specjalistów z zakresu cyberbezpieczeństwa. Aby skutecznie przygotować studentów do pracy w tej specyficznej i wymagającej dziedzinie, konieczne jest zidentyfikowanie luk kompetencyjnych oraz określenie kluczowych umiejętności niezbędnych na współczesnym rynku pracy.

Podsumowując, student uzyskuje wiedzę specjalistyczną związaną z rozwiązaniami CISCO, natomiast ta wiedza jest uzupełniana o wiedzę ogólną poprzez przedmioty kierunkowe i modułowe. W ten sposób absolwent ma kompetencje typowe dla podejścia zwinnego w kształcie litery T, to znaczy w jednej dziedzinie jest specjalistą, w pozostałych posiada wiedzę ogólną.

ZARZĄDZANIE BEZPIECZEŃSTWEM I AUDYTY BEZPIECZEŃSTWA

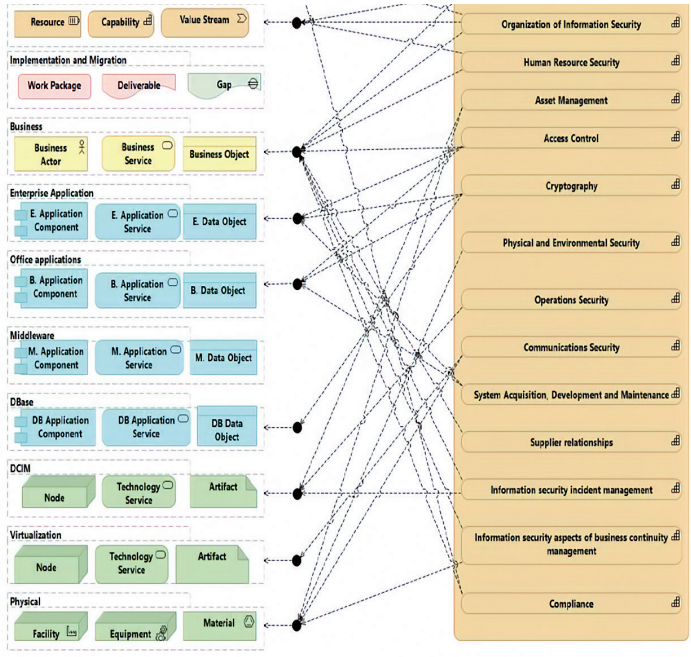
Naturalnym sposobem rozwiązywania problemów bezpieczeństwa w firmach jest wybranie i przestrzeganie uznanych standardów bezpieczeństwa. Wiąże się to jednak z następującymi pytaniami: jakie standardy

bezpieczeństwa powinny być stosowane i w jakim zakresie; w jakim stopniu stosowanie standardów eliminuje luki w bezpieczeństwie; czy stosowanie standardów znacząco ogranicza (spowalnia) działalność firmy; czy istnieje rozwiązanie, które nie wymagałoby dużych funduszy i ludzi, aby zapewnić zgodność z tymi standardami; wreszcie, jak obiecujące są wybrane rozwiązania dla przyszłości zarządzania bezpieczeństwem. Standardy bezpieczeństwa zapewnia się poprzez budowę systemu ISMS (Information Security Management System). Jedną z podstawowych kwestii w tym zakresie jest określenie, w jakim stopniu standardy bezpieczeństwa spełniają potrzeby bezpieczeństwa przedsiębiorstw.

Popularną rodziną norm, które ułatwiają zarządzanie bezpieczeństwem w organizacji dowolnego rodzaju dla wszystkich rodzajów zasobów informacyjnych są normy ISO / IEC 27000. W ramach tej grupy norm najbardziej powszechne są:

- Norma ISO/IEC 27000:2018 (Information technology – Security techniques – Information security management systems – Overview and vocabulary) [8], która definiuje ISMS i słownictwo używane w tej rodzinie norm.
- Norma ISO/IEC 27001:2013 [9], która definiuje wymagania dla ISMS. Norma ISO 27001 dzieli praktyki bezpieczeństwa na 14 domen kontroli (od 5 do 18). Rys. 1 przedstawia niektóre powiązania praktyk z aktywami przedsiębiorstwa.
- Norma ISO/IEC 42001:2023 określa wymagania dotyczące ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia Systemu Zarządzania Sztuczną Inteligencją (AIMS) w organizacjach. Jest ona przeznaczona dla podmiotów dostarczających lub wykorzystujących produkty lub usługi oparte na AI, zapewniając odpowiedzialny rozwój i użytkowanie systemów AI. Do celów normy ISO/IEC 42001 zaliczyć można m.in.: zachęcanie firm, aby podczas opracowywania i wdrażania sztucznej inteligencji traktowały dobro ludzi, bezpieczeństwo i doświadczenia użytkowników jako priorytet; pomaganie organizacjom w przestrzeganiu odpowiednich przepisów prawnych dotyczących ochrony danych lub obowiązków wobec zainteresowanych stron.

Rys. 1. Odwzorowanie ISO27001 na aktywa firm



Źródło: opracowanie własne.

Na Rys. 1 przedstawiono wszystkie aktywa przedsiębiorstwa w języku modelowania architektury korporacyjnej ArchiMate. W języku tym wyróżnia się następujące warstwy przedsiębiorstwa: motywacji, strategii, implementacji i migracji, a także podstawowe warstwy, którymi są: warstwa biznesowa, aplikacji, techniczna (infrastruktury) oraz warstwa fizyczna. Na rysunku zestawiono powiązania 14 domen bezpieczeństwa z elementami architektury przedsiębiorstwa. Ten sposób przedstawienia pozwala uzyskać całościowe (holistyczne) spojrzenie na normę i systemy IT dla których będą budowane strategie bezpieczeństwa.

BEZPIECZEŃSTWO SYSTEMÓW W ORGANIZACJACH IT/OT

Standardy bezpieczeństwa IT nie zawsze są odpowiednie dla środowisk OT (technologii operacyjnych). Systemy OT mają m.in. różne wymagania

dotyczące wydajności i dostępności oraz żywotności sprzętu. Co więcej, cyberataki na systemy informatyczne mają zasadniczo konsekwencje gospodarcze, podczas gdy cyberataki na infrastrukturę krytyczną mogą również mieć poważny wpływ na środowisko, a nawet zagrażać zdrowiu i życiu publicznemu. Infrastruktura i konfiguracja OT opierają się często na definicjach i wymaganiach, które różnią się od wymagań infrastruktury przedsiębiorstwa. Infrastrukturę OT powinna m.in. cechować: wysoka dostępność, zabezpieczenia konstrukcyjnie, solidność, determinizm, szybka i prosta wymiana poszczególnych elementów, łatwość podłączenia do firmowego IT, uwzględnienie standardów bezpieczeństwa stosowanych w branży.

Infrastruktura i architektura OT powinny być ustandaryzowane (standaryzacja nie powinna zwiększać złożoności), dostosowane do istniejących maszyn, systemów i procesów, bezproblemowo integrować się z korporacyjnym IT. Infrastruktura OT umożliwia personelowi bez kompetencji IT do obsługi i konserwacji maszyn i procesów, niezależnie od lokalizacji możliwość dostępu do danych, dostosowanie do potrzeb firmy i jednocześnie elastyczność cyfryzacji. W rozwiązaniach IT/OT proponowane są następujące standardy:

NIST 800-82. Standard został stworzony w celu zapewnienia większej przejrzystości stosowania nowoczesnych strategii ograniczania ryzyka IT w świecie pozornie izolowanych urządzeń ICS, które są coraz częściej migrowane do infrastruktury IT. Celem tego standardu jest ograniczenie obszaru, na którym cyberprzestępczość może atakować podmioty infrastruktury krytycznej, takie jak, wytwórnie energii, producenci produktów farmaceutycznych, czy żywności. Standard NIST 800-82 ICS obejmuje: serwery proxy, segregację, monitorowanie, rejestrowanie i stosowanie protokołów bezpieczeństwa w ICS oraz ocenę zagrożeń stwarzanych przez ICS, które zwiększają się wraz z łącznością internetową.

IEC 62443. Seria norm IEC 62443 została opracowana w celu ochrony systemów automatyki przemysłowej i sterowania. Obecnie obejmuje dziewięć norm, raportów technicznych i specyfikacji technicznych i dotyczy nie tylko technologii systemu sterowania, ale także procesów pracy, środków zaradczych i pracowników. W normie przyjęto podejście całościowe, ponieważ nie wszystkie zagrożenia mają charakter technologiczny. W tej normie przyjęto podejście oparte na ryzyku, w oparciu o koncepcję, że próba jednakowej ochrony wszystkich zasobów nie jest ani skuteczna, ani trwała. Zamiast tego użytkownicy muszą zidentyfikować to, co jest najcenniejsze i najbardziej podatne na ataki, oraz zidentyfikować słabe punkty, co w końcu doprowadzi do zbudowania architektury obronnej zapewniającej ciągłość działania.

PERA (Purdue Enterprise Reference Architecture). Model Architektury IT/OT Purdue został opracowany jako model referencyjny komputerowo zintegrowanej produkcji (CIM) dla całkowicie zautomatyzowanych procesów. Model ten został wprowadzony przez Theodora Wiliamsa i konsorcjum Uniwersytetu Purdue w roku 1992. Model ten pomimo tego, że jest dosyć stary to nadal spełnia wymagania segmentacji jako podstawowego rozwiązania w sferze bezpieczeństwa, zarówno sieci bezprzewodowych, jak i przewodowych oraz chroni sieć OT (Segmentacja może bazować na izolacji poszczególnych warstw). Model referencyjny Purdue jest modelem do systemów SCADA, obejmuje on 7 podstawowych warstw funkcjonalnych systemu (Rys. 2). Model Purdue oferuje szereg korzyści w zakresie zabezpieczania środowisk ICS:

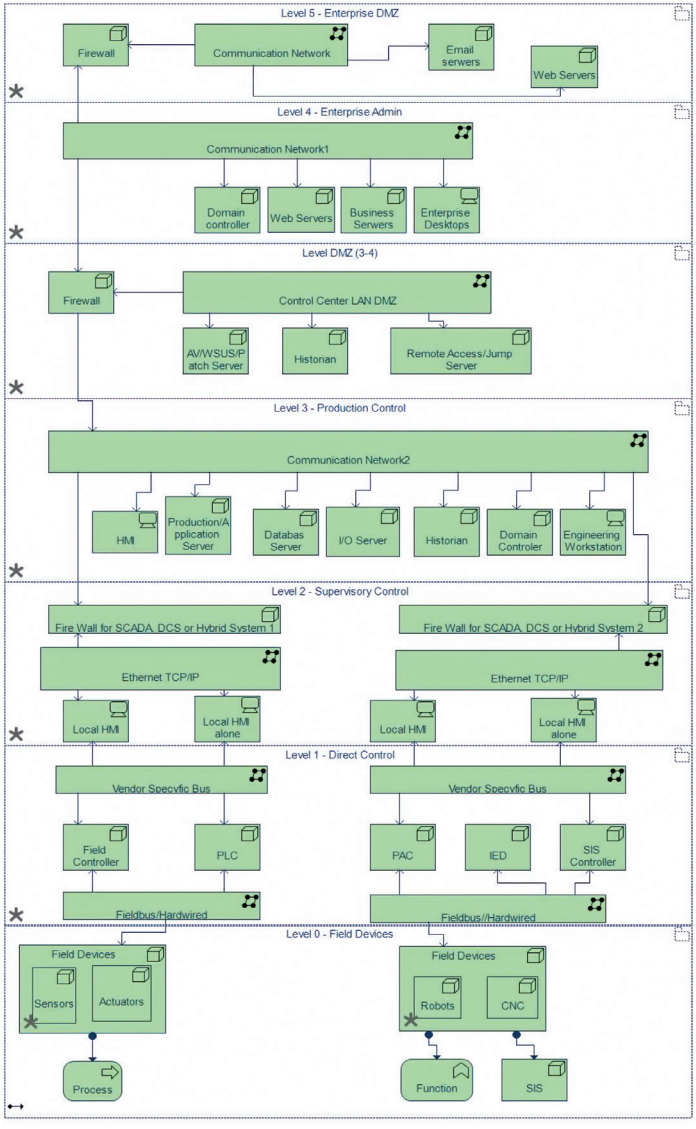
- Jasna segmentacja: Zapewnia jasne granice i separację między różnymi poziomami, umożliwiając wdrożenie odpowiednich kontroli bezpieczeństwa na każdym poziomie.
- Skalowalność: Hierarchiczna natura modelu umożliwia skalowalność i elastyczność w zabezpieczaniu środowisk ICS, dostosowując się do różnych architektur i rozmiarów systemów.
- Wspólny język: Model Purdue ustanawia wspólny język i ramy komunikacji między systemami IT i OT, zapewniając wspólne zrozumienie wymagań bezpieczeństwa

Model PERA tworzy przejrzyste struktury komunikacji i zależności pomiędzy systemami i może stanowić podstawę do segmentacji przemysłowych sieci sterowania. Dzięki jasnemu wyznaczeniu i zabezpieczeniu stref można wdrożyć odpowiednie koncepcje bezpieczeństwa IT i OT. Oto jak model PERA widziany jest przez Zscaler, jednego z najpopularniejszych dostawców w sferze Zero Trust Cybersecurity, przedstawiono w [10]:

Wszystkie 3 standardy mają zastosowanie w architekturach organizacji i przedsiębiorstw przemysłowych [11]. To, który model będzie odpowiedni zależy od wielu czynników, takich jak, istniejąca już infrastruktura, możliwości dostosowania nowych technologii do przyszłościowych rozwiązań w domenie Zero Trust oraz od strony finansowej (która zawsze jest priorytetowa dla decydentów).

Rys 2. przedstawia propozycję adaptacji modelu PERA pod kątem bezpieczeństwa z uwzględnieniem segmentacji i integracji. Model ten zawiera poziomy od 0 do 5 i został opracowany w języku ArchiMate przeznaczonym do modelowania i wizualizacji architektur korporacyjnych. W modelu tym ograniczono się do przedstawienia warstwy technicznej z wykorzystaniem głównie konceptu węzłów języka ArchiMate.

Rys 2: Opis poziomów OT systemu PERA pod kątem bezpieczeństwa (Opracowanie własne)



Źródło: opracowanie własne.

Jednym ze sposobów segmentacji jest tworzenie stref zdemilitaryzowanych DMZ (Demilitarized Zone). W wojskowości oznacza to obszar, w którym nie mogą być prowadzone działania militarne. Podstawowe funkcje DMZ to zapewnienie bezpieczeństwa (chroni wewnętrzne zasoby organizacji, takie jak, serwery baz danych, wewnętrzne aplikacje i inne krytyczne systemy, przed bezpośrednim dostępem z zewnątrz), izolacja (tworzy izolowaną przestrzeń w sieci, gdzie można umieścić serwery, które muszą być publicznie dostępne, takie jak serwery WWW, serwery pocztowe, serwery FTP czy serwery DNS, bez ryzyka dla wewnętrznej sieci firmowej), kontrola dostępu (stosowane są szczególne zasady kontroli dostępu, które precyzyjnie regulują, kto i jak może się łączyć z usługami w tej strefie, oraz jak dane mogą przepływać pomiędzy DMZ a siecią wewnętrzną).

Poziom 0. Urządzenia polowe (Field Devices). Są to komponenty potrzebne do rzeczywistych fizycznych procesów produkcyjnych. Dostarczają dane procesowe do sterowników poziomu 1 i przyjmują od nich polecenia. Typowe komponenty tego poziomu obejmują: czujniki (temperatura, światło, wilgotność...), siłowniki (silniki, zawory...), maszyny (CNC, roboty...). W tradycyjnych rozwiązaniach na tym poziomie zazwyczaj nie stosowane są mechanizmy bezpieczeństwa. Zabezpieczenia te są istotne w krytycznych strukturach, takich jak, elektrownie, zakłady chemiczne i inne. Czasami te urządzenia stanowią pierwszą linię obrony dzięki zastosowanym rozwiązaniom bezpieczeństwa, w tym inteligentnych czujnikach, segmentacji sieci.

Poziom 1. Sterowanie bezpośrednie (Direct Control). Poziom ten jest też nazywany jako poziom sterowania urządzeniami (Device Control Level), poziom sterowania w czasie rzeczywistym (Real-time Control Level), poziom sterowania procesem (Process Control Level). Poziom ten zawiera urządzenia (sterowniki, kontrolery), które odbierają dane procesowe z urządzeń (np. czujników) z poziomu 0 i sterują tymi urządzeniami. Typowe komponenty to: urządzenia polowe (Field Device), rozproszone systemy sterowania (DCS Distributed Control System), programowalne sterowniki logiczne (PLC Programmable Logic Controller), zdalne terminale (RTU – Remote Terminal Unit), Kontroler Systemu Instrumentacji Bezpieczeństwa (Safety Instrumented System (SIS) Controller, Programowalny Kontroler Automatyzacji (PAC – Programmable Automation Controller), Inteligentne Urządzenie Elektroniczne (IED – Intelligent Electronic Device). Łączność Ethernet/IP jest rzadkością w tym obszarze, jednakże ze względu na interoperacyjność i standaryzację w tej strefie, starsze protoko-

ły są coraz częściej zastępowane przez Ethernet/IP. Poziomy 0 i 1 komunikują się zazwyczaj poprzez połączenia dwuprzewodowe i linie szeregowe. Niektóre procesy produkcyjne wymagają (izochronicznej) komunikacji w czasie rzeczywistym pomiędzy tymi poziomami. Aby zagwarantować prawidłowe działanie, nie może być żadnych przerw ani opóźnień (np. w sterowaniu silnikiem krokowym). Środki bezpieczeństwa na tym poziomie obejmują kontrole dostępu i ochronę przed nieautoryzowanymi modyfikacjami.

Poziom 2. Sterowanie nadzorcze (Supervisory Control). Poziom obejmuje operacje i kontrole produkcji w zakładzie. Typowymi komponentami w tym obszarze są: systemy SCADA (Supervisory Control and Data Acquisition), Interfejsy człowiek-maszyna (HMI), stanowiska operatorskie, kontrola nadzorcza i pozyskiwanie oraz wizualizacja danych. Ta strefa obejmuje urządzenia monitorujące i sterujące dla pojedynczego obszaru/komórki produkcyjnej. Należą do nich takie elementy jak: serwery aplikacji, serwery bazy danych, serwery plików, centralne usługi sieciowe (DNS, DHCP, NTP, Active Directory), inżynierskie stanowiska pracy. Poziom ten może być podporządkowany systemowi kontroli SCADA lub DCS (Distributed Control System) lub może występować forma hybrydowa tych 2 systemów.

Poziom 3. Zarządzanie produkcją (Production Control). Systemy tego poziomu 3 zarządzają, monitorują i kontrolują pracę zakładu w zakresie globalnym (w przypadku poziomu 2 to jest zakres lokalny). Typowe komponenty na tym poziomie to: archiwizator danych (data, historia), który rejestruje i nagrywa działanie serwerów, czy np. pliki projektu, określających zachowanie sterowników, stanowiska operatorskie (na poziomie zakładu), systemy planowania zasobów (ERP). Do sfery bezpieczeństwa na tym poziomie zaliczyć trzeba zapobieganie nieautoryzowanemu dostępowi, czy zapewnienie integralności danych.

Poziom 3-4 DMZ (Demilitarized Zone – strefa zdemilitaryzowana). Poziom ten występuje ze względów bezpieczeństwa i polega na oddzieleniu sieci zakładowej (Głównie sieci OT od zewnętrznych sieci publicznych). Jest to dodatkowa ochrona zmniejszająca ryzyko cyberataków i nieautoryzowanego dostępu do sieci zakładowych, tzw. wewnętrzny DMZ. Na tym poziomie może zostać zainstalowany archiwizator danych (data, historia), który służy do gromadzenia, przechowywania, kompresji i agregacji oraz do analizowania danych procesowych z systemów automatyki przemysłowej w czasie rzeczywistym. Na tym poziomie mogą być instalowane (aczkolwiek coraz rzadziej) tzw. jump servery. Mają one za zadanie umożliwić

klientom, względnie pracownikom firm zewnętrznych zdalny dostęp do sieci poprzez bezpieczne ominięcie firewallu.

Poziom 4. Zarządzanie firmą (Enterprise Admin). Tutaj odbywa się planowanie biznesowe i logistyka obiektu. Poziom ten obejmuje systemy informatyczne związane z procesami OT służące do planowania zasobów i monitorowania/kontrolowania procesu produkcyjnego. Typowe komponenty obejmują: oprogramowanie do planowania zasobów przedsiębiorstwa (ERP), systemy realizacji produkcji (MES), serwery internetowe. Poziom ten reprezentuje tradycyjną sieć IT zawierającą min. urządzenia IT, takie jak serwery uwierzytelniające, komputery stacjonarne dla przedsiębiorstw, wewnętrzną bazę danych i serwery plików.

Poziom 5. DMZ firmy (Enterprise DMZ). Poziom ten obejmuje komponenty IT, które są publicznie dostępne w Internecie (web serwery, e-mail serwery) i dlatego wymagają szczególnej ochrony. Typowe komponenty obejmują: serwery proxy, bramy VPN, bramy e-mailowe. Bezpieczeństwo na tym poziomie to przede wszystkim ochrona żywotnych informacji biznesowych oraz wdrożenie systemów odpowiedzialnych za cyberbezpieczeństwo.

W praktyce podział na warstwy jest dostosowywany do potrzeb firm. Kuriozalnie obecnie zaczyna się już usuwać niektóre między-warstwy, bo najnowsze technologie nie potrzebują jakichś ekwilibrystycznych rozwiązań w sferze bezpieczeństwa jak np. Jump Servery. Chociaż tego w modelu nie wyróżniono, to można mówić także o warstwie integracji, która umożliwia łatwy przepływ danych pomiędzy systemami. Celem warstwy integracji jest zjednoczenie systemów IT i OT, standaryzacja danych i komunikacji, bezpieczna i wydajna wymiana danych,

WYBRANE METODY ZAPEWNIENIA BEZPIECZEŃSTWA SYSTEMÓW IT/OT

Najpopularniejszą i sprawdzoną metodą na uzyskanie minimum bezpieczeństwa systemów IT/OT jest przeprowadzenie segmentacji. W systemach OT występuje dążenie do konwergencji systemów, a jednocześnie stosuje się segmentację, by zapewnić odpowiedni poziom bezpieczeństwa. Przeprowadzając segmentację w architekturze IT/OT, należy od początku wziąć pod uwagę także negatywne skutki, jakie może przynieść ze sobą ta metoda. Segmentacja i tak zwana nadmierna segmentacja mogą prowadzić między innymi do problemów z wydaj-

nością. Przeprowadzenie segmentacji IT/OT może się składać z następujących etapów:

1. Określenie celów segmentacji (zwiększenie bezpieczeństwa systemów czy poprawa wydajności operacyjnej).
2. Przeprowadzenie audytu systemów IT/OT. Jakie urządzenia, aplikacje i systemy są używane w organizacji i jak są one połączone.
3. Wyznaczenie granic segmentacji. Określenie, które systemy powinny być odseparowane od siebie.
4. Dobór odpowiednich narzędzi i technologii.
5. Wdrożenie segmentacji w sposób stopniowy i kontrolowany.
6. Monitorowanie i utrzymywanie. Systemy należy monitorować w celu sprawdzenia czy działają poprawnie. Utrzymanie może polegać na aktualizowaniu systemów i narzędzi, w celu zapewnienia bezpieczeństwa i skuteczności działania.

Zasadniczo istnieją cztery różne typy segmentacji sieci:

1. Segmentacja galwaniczna, która oznacza całkowite oddzielenie sieci w celu zapobiegania potencjalnemu przeniesieniu spowodowanemu na przykład uderzeniem pioruna lub awarią elementu elektrycznego. Między innymi połączenie sieciowe redundantnych komponentów powinno wówczas odbywać się za pomocą światłowodów.
2. Segmentacja fizyczna, która dotyczy sytuacji, gdy dwie sieci komunikują się ze sobą wyłącznie za pośrednictwem oddzielającej instancji zabezpieczeń (zwykle firewall), a sieci nie są ze sobą dalej połączone z wyjątkiem instancji oddzielającej.
3. Segmentacja logiczna (zoning – segmentacja sieci), która opiera się na kilku wzajemnie połączonych technologiach i konfiguracjach: podsieciach, sieciach VLAN oraz fizycznych i wirtualnych strefach bezpieczeństwa. Podstawą prawidłowego i skutecznego zoningu jest określenie zakresu usług oraz urządzeń na których są one zainstalowane. W pierwszej fazie segmentacji sieć dzielona jest na podsieci. Każda z nich ma przyporządkowane inne urządzenia, które przypisane są poszczególnym logicznym grupom. Jedna podsieć przeznaczona jest dla serwerów, druga do rozliczania, a jeszcze inna do zarządzania siecią. Domyślnie zdefiniowane są osobne podsieci do rejestrowania i monitorowania, a inne do zarządzania obiektami firmy. Możliwe są ustawienia i osobne uprawnienia dla każdego urządzenia i aplikacji. Określa się, kto i z kim może się kontaktować. Na przykład, kto ma dostęp do Internetu, a kto nie. Następnie definiowane są sieci VLAN, a na koniec przydzielane są adresy IP do

sieci VLAN. Schemat adresowania IT i przypisanie sieci VLAN stanowią ostateczny poziom segmentacji. Przy tworzeniu całościowego obrazu sieci IT i połączeń w niej zachodzących powinno posłużyć się różnymi typami macierzy adresów IP.

4. Mikrosegmentacja, która jest stosowana w przypadkach, gdy istnieje znaczne zagrożenie bezpieczeństwa pojedynczego urządzenia OT (z niezabezpieczonym oprogramowaniem lub systemem operacyjnym podłączonym do systemu centralnego) dla innych podłączonych komórek lub całego terenu fabryki. Może to być na przykład niechronione urządzenie, które musi komunikować się za pomocą niezabezpieczonych protokołów z wieloma innymi urządzeniami w zakładzie (np. poprzez FTP, HTTP, MQTT...). Przed zabezpieczeniem takich urządzeń poprzez mikrosegmentację, należy przeprowadzić odrębną analizę ryzyka.

Oprócz opisanych powyżej metod segmentacji, mających zapewnić bezpieczeństwo infrastruktury przedsiębiorstwa, należy dodatkowo przeprowadzić działania, które podniosą poziom bezpieczeństwa systemów IT/OT. Jednakże same te dodatkowe zabezpieczenia bez uprzedniej segmentacji nie gwarantują odpowiedniej ochrony przeciw np. cyberatakami.

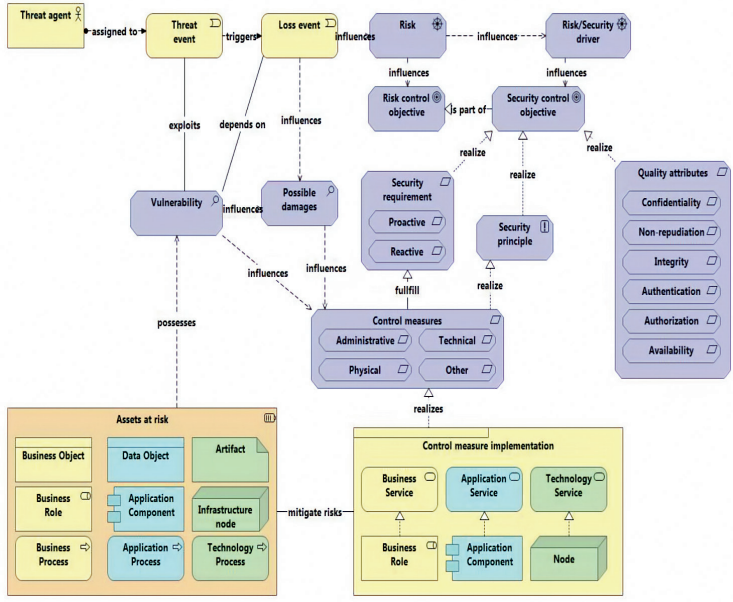
HOLISTYCZNE MODELE BEZPIECZEŃSTWA W ORGANIZACJACH IT/OT

Przedsiębiorstwo IT/OT możemy potraktować jako całość i opisać przy użyciu architektury korporacyjnej. Dla takiego rodzaju przedsiębiorstw celowe jest opracowanie modeli referencyjnych bezpieczeństwa cyfrowego przedsiębiorstw [12]. Celem tych modeli jest spojrzenie na bezpieczeństwo jako całość i w tym celu użyto języka architektury korporacyjnej do opisania całego spektrum zagadnień związanych z bezpieczeństwem. Bezpieczeństwo i ryzyko muszą być traktowane razem w modelu architektury korporacyjnej, jak pokazano w [13]. Meta-model ISSRM (Information System Security Risk Management) został przedstawiony na Rys. 3. Zastosowano język ArchiMate, który jest dobrym rozwiązaniem do modelowania architektury korporacyjnej, ryzyka korporacyjnego i bezpieczeństwa [14]. Niektóre publikacje w „The Open Group" omawiają sposób modelowania zarządzania ryzykiem korporacyjnym i bezpieczeństwa przy użyciu języka ArchiMate [15], [16]. W modelu wprowadzono następujące pojęcia (Rys.3):

- Zagrożenie (Threat) – możliwe niebezpieczeństwo, które może wykorzystać lukę systemu i spowodować potencjalne szkody:
  - Agent zagrażający (Threat agent) – wszystko to (np. osoba, organizacja lub przedmiot), co może spowodować uszkodzenie aktywów.
  - Zdarzenie zagrażające (Threat event) – zdarzenie, które może niekorzystnie wpłynąć na aktywa.
  - Zdarzenie powodujące stratę (Loss event) – okoliczności powodujące stratę lub uszkodzenie składnika aktywów.
- Podatność (Vulnerability) – rozumiana jako słabość elementów systemu, czyni system podatnym na zagrożenia.
- Ryzyko (Risk) to coś, co może powodować problemy lub straty.
  - Motywator ryzyka/bezpieczeństwa (risk / security driver) reprezentuje stan, który motywuje organizację do wdrożenia zmian mających na celu osiągnięcie celów w zakresie ryzyka i bezpieczeństwa.
  - Cele kontroli ryzyka i bezpieczeństwa (Risk and security control) opisują zasady i procedury, które należy ustanowić dla skutecznych strategii ryzyka.
- Wymogi bezpieczeństwa określają, jakie środki kontroli należy wybrać, aby spełnić te wymagania.
- Zasada bezpieczeństwa – ogólna właściwość stosowana w systemie (np. polityka).
- Aktywa zagrożone (Asset at risk) – wszystko, co materialne lub niematerialne, które ma wartość lub wytwarza wartość.
- Wdrażanie środków kontrolnych – stosowanie polityk i procedur.

Takie podejście ułatwia rozumienie zagadnień bezpieczeństwa IT i OT. W tym modelu występuje jednakowe podejście do bezpieczeństwa IT i OT bazujące na ryzyku.

Rys. 3. Meta model ryzyka



Źródło: zaadaptowane na podstawie [13].

Identyfikacja luk kompetencyjnych oraz rozwój kluczowych umiejętności w kontekście IT/OT to fundamentalne zadanie dla uczelni kształcących przyszłych specjalistów ds. cyberbezpieczeństwa. Poprzez dostosowanie programów nauczania do wymagań rynku oraz specyfiki zintegrowanych środowisk IT/OT, uczelnie mogą skutecznie przygotować swoich absolwentów do pracy w jednej z najbardziej wymagających, ale i kluczowych dziedzin współczesnej gospodarki.

PODSUMOWANIE

Kształcenie specjalistów na studiach z zakresu cyberbezpieczeństwa wymaga dobrego dopasowania kompetencji do potrzeb różnych firm. Ze względu na okres trwania studiów, rozwinięte zostaną tylko wybrane kompetencje. Przedsiębiorstwo zatrudniające absolwentów musi sobie zdawać sprawę z luki kompetencyjnej. Wyznaczenie tej luki kompeten-

cyjnej powinno prowadzić do ukierunkowanych działań w przedsiębiorstwach w zakresie rozwoju kompetencji minimalizujących ryzyko strat związanych z cyberbezpieczeństwem. W niniejszym artykule przedstawiono propozycję programu kształcenia, dzięki któremu studenci zdobywają wiedzę specjalistyczną bazującą na kursach i certyfikatach CISCO. Dodatkowo proponowane są zajęcia, które umożliwiają zdobycie wiedzy ogólnej. Absolwent będzie posiadał w jednym obszarze głęboką wiedzę specjalistyczną (specialist), a w pozostałych wiedzę ogólną (generalist).

Istnieje kilka możliwości uzupełnienia wiedzy i umiejętności z zakresu bezpieczeństwa systemów. Jedną z takich możliwości są laboratoria projektowe, gdzie studenci mogą zdobywać wiedzę i umiejętności rozwiązując konkretne problemy. Kolejnym rozwiązaniem ułatwiającym likwidację luk kompetencyjnych są praktyki oraz zatrudnianie studentów (zwykle będących w końcowej fazie studiów) w charakterze tzw. studentów pracujących. Takie „wdrożenie" w życie zawodowe studentów ma wiele pozytywnych stron. Nowo uzyskaną wiedzę sprawdza się w działaniach praktycznych, takich jak projekty, czy administrowanie systemami informatycznymi. „Learning by doing" jest naczelną zasadą przy zatrudnianiu „pracującego studenta".

Firmy zatrudniające studentów często umożliwiają im zdobywanie certyfikatów od wiodących dostawców IT (MS Azure, Cisco Systems CCNA itp.). Korzyści z takiego rozwiązania są obopólne. Student rozwija wiedzę praktyczną i sprawdza zdobytą teorię, a firmy budują swoich wieloletnich ekspertów, których się szkoli i wdraża we własnych strukturach. Student może posiąść różne umiejętności podczas takiej pracy, jak: przetwarzanie w chmurze, administrowanie sieciami LAN, WAN, TCP/IP, Modbus; znajomość bezpieczeństwa IT zgodnie ze standardami bezpieczeństwa (np. ISO 27001); znajomość Windows, (Active Directory), Linux, SQL, SharePoint i innych narzędzi/aplikacji; praktyczne umiejętności w administrowaniu VMware, vSphere; podstawowa znajomość koncepcji automatyzacji i systemów automatyzacyjnych (np. UC4, Jira); podstawowa znajomość frameworku ITIL; znajomość technologii sieciowych takich jak: Fortinet, Netscaler, Cisco Systems, Mimecast, Linux; praktyczna znajomość Microsoft Server 2019 HyperV, klaster pracy awaryjnej, usługi Azure, pamięć masowa i FibreChannel, systemy monitorowania i tworzenia kopii zapasowych.

Podsumowując możemy stwierdzić, że dobrym rozwiązaniem jest kształcenie studentów na specjalistów w jednym obszarze, a w pozostałych ważne jest posiadanie kompetencji ogólnych. Ten rodzaj podziału kompetencji jest zalecany dla członków zespołów zwinnych. Ważne jest

by zdawać sobie sprawę z luk kompetencyjnych w innych obszarach bezpieczeństwa. Taką świadomość uzyskuje się przy zdobywaniu wiedzy ogólnej. Następnym krokiem jest likwidacja luk kompetencyjnych zgodnie z potrzebami przedsiębiorstw.

LITERATURA

1. Amit.Musale (2022) *Top 7 OT Cyber-attacks That Decimated Businesses.* In: Payatu. https://payatu.com/blog/ot-attacks/. Accessed 15 Aug 2024.
2. Santos, Omar (2020) *Cisco CyberOps Associate* CBROPS 200-201 Official Cert Guide.
3. Rios RG, Hucaby D (2020) *CCNP Enterprise Core ENCOR 350-401 and Advanced Routing ENARSI 300-410* Official Cert Guide Library.
4. Gooley J, Jackson C (2020) *Cisco Certified DevNet Associate DEVASC* 200-901 Official Cert Guide.
5. ENCOR Exam Topics. https://learningnetwork.cisco.com/s/encor-exam-topics. Accessed 15 Aug 2024.
6. CBROPS Exam Topics. https://learningnetwork.cisco.com/s/cbrops=-exam-topics?ccid=cyberopsassociate&dtid=website&oid-cdc-cyberopsassociate-rec-training. Accessed 15 Aug 2024.
7. DevNet Associate Exam Topics. https://learningnetwork.cisco.com/s/devnet-associate-exam- topics. Accessed 15 Aug 2024.
8. ISO – International Organization for Standardization ISO/IEC 27000:2018. In: ISO. https://www.iso.org/cms/render/live/en/sites/iso-org/contents/data/standard/07/39/73906.html. Accessed 27 Dec 2020.
9. ISO – International Organization for Standardization ISO/IEC 27001:2013. In: ISO. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html. Accessed 27 Dec 2020.
10. ENGINEER M (2023) *The Purdue Model of Security for Manufacturing: Safeguarding Industrial Control Systems.* https://www.mesengineer.com/2023/08/20/the-purdue-model-of-security-for- manufacturing--safeguarding-industrial-control-systems/. Accessed 15 Aug 2024.
11. Cybersecurity in Industrial Control Systems: *An integration of information technology and operational technology*. https://ieeexplore--1ieee-1org- 1000047xe001f.wbg2.bg.agh.edu.pl/document/9968468. Accessed 18 Aug 2024.

12. Urbanczyk W, Werewka J (2021) *Application of a Government Data Center (GDC) Reference Model for Security Management Analysis.* In: IEEE International Conference on e-Business Engineering, ICEBE 2021, Guangzhou, China, November 12-14, 2021. IEEE, pp 112–119
13. Jonkers H, Quartel DAC (2016) *Enterprise Architecture-Based Risk and Security Modelling and Analysis. In: Kordy B, Ekstedt M, Kim DS (eds) Graphical Models for Security.* Springer International Publishing, Cham, pp 94–101.
14. Modelling Security Aspects with ArchiMate: A Systematic Mapping Study. https://ieeexplore-1ieee-1org-1000047xe001f.wbg2.bg.agh.edu.pl/document/9226325. Accessed 18 Aug 2024.
15. Band I, Engelsman W, Feltus C, et al (2015) *Modeling enterprise risk management and security with the ArchiMate Language.*
16. The Open Group (2019) *How to Model Enterprise Risk Management and Security with the ArchiMate® Language.* https://publications.opengroup.org/white-papers/archimate/w172. Accessed 30 Dec 2020.