Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla zarządzających		
Część 1, Tydzień 2 **Moduł: Wprowadzenie do webinarium**		
Zajęcia edukacyjne	❑ **Webinarium** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑**Prezentacja** ❑ **Inne**	
Odpowiedzialni za zajęcia	Gabriel Vladut Valentin Istratie	
Cele aktywności edukacyjnej	1. Wprowadzenie do projektu Erasmus+ InCyT 2. Cyberbezpieczeństwo 3. Pojęcia, definicje i terminy 4. Standardy kontroli wewnętrznej 5. Opracowanie kontroli bezpieczeństwa cybernetycznego	
Umiejętności do zdobycia	• TS3 Bezpieczeństwo sieci • Testy penetracji TS4 (luki w zabezpieczeniach) • SS3 Analiza poznawcza i behawioralna	
Czas trwania okresu edukacyjnego	2 tygodnie	
Wymagania wstępne	***Co jest potrzebne?***	
	• Wiedza i świadomość dotycząca cyberbezpieczeństwa, czym są ataki na cyberbezpieczeństwo • Metody zapobiegania naruszeniom danych wykorzystywanych przez atakujących w celu uzyskania dostępu do wrażliwych danych i wykorzystania luk w organizacji • Postępowanie w przypadku ataku cyberbezpieczeństwa	

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Description
Zapewnienie bezpieczeństwa informacji jest kluczowe. Systemy kontroli wewnętrznej są ważne, a ich brak bardzo często stanowi zagrożenie dla cyberbezpieczeństwa. Ochrona informacji i systemów informatycznych obejmuje ochronę przed nieuprawnionym dostępem lub modyfikacją informacji podczas przechowywania, przetwarzania lub przesyłania, a także przed odmową usługi upoważnionym użytkownikom. Bezpieczeństwo informacji obejmuje środki niezbędne do wykrywania, dokumentowania i przeciwdziałania takim zagrożeniom. Bezpieczeństwo informacji składa się z bezpieczeństwa komputerowego i bezpieczeństwa komunikacji(zwane także jako INFOSEC). Obejmuje pojęcia jak: bezpieczeństwo komunikacji; bezpieczeństwo komputera; bezpieczeństwo informacji; System informacyjny. Kontrole wewnętrzne są stosowane przez kierownictwo, bezpieczeństwo IT, zespoły finansowe, księgowe i operacyjne, aby osiągnąć zapewnienie wiarygodności i dokładności informacji finansowych. Kontrole wewnętrzne zapewniają, że dokładne, aktualne i kompletne informacje znajdują odzwierciedlenie w rachunkowości systemu i raportach finansowych. Uczestnicy kursu będą informowani o takich aspektach, czytając odpowiedni tekst, oglądając webinaria i rozwiązując ćwiczenia we własnym tempie. Wszystkie te dokumenty znajdują się na cyfrowej interaktywnej platformie projektowej. Kursanci mogą przetestować swoje odpowiedzi wykonując quizy. Odpowiedzi na inne ćwiczenia należy zapisać na odpowiednim forum dyskusyjnym i przedyskutować z mentorem na wspólnym zorganizowanym spotkaniu raz w tygodniu. Kursant może współpracować z innymi osobami i mentorem, szczególnie podczas spotkań. Będą one wspierane w celu opracowania e-portfolio ważnego dla refleksji i oceny szkolenia.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Treść materiału edukacyjnego

Opis

Bezpieczeństwo informacji

Bezpieczeństwo informacji dotyczy ochrony informacji i systemów komputerowych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, przerwaniem, modyfikacją lub zniszczeniem.

ISO/IEC27002/2013 definiuje bezpieczeństwo informacji poprzez trzy główne elementy: poufność, integralność i dostępność. Poufność zapewnia szyfrowanie informacji. Integralność osiąga się dzięki mechanizmom i algorytmom rozpraszania.

Dostępność zapewnia wzmocnienie bezpieczeństwa sieci lub sieci systemów komputerowych oraz tworzenie kopii zapasowych. Bezpieczeństwo informacji to zestaw praktyk zaprojektowanych w celu ochrony danych.

Bezpieczeństwo informacji nie ogranicza się do systemów komputerowych lub informacji w formie cyfrowej lub elektronicznej. Dotyczy wszystkich spraw związanych z bezpieczeństwem, ochroną danych lub informacji, niezależnie od ich formy.

Bezpieczeństwo informacji nie może być zdefiniowane jako synonim bezpieczeństwa komputera, bezpieczeństwa systemu i sieci, bezpieczeństwa technologii informacyjnej, systemów informatycznych lub technologii teleinformatycznych. Każde z tych wyrażeń odnosi się do innego tematu, nawet jeśli punkt wspólny dotyczy bezpieczeństwa informacji w niektórych jego formach (tu mówimy o jego wersji elektronicznej), dlatego wszystkie są poddziedzinami bezpieczeństwa informacji.

W XXI wieku większość organizacji posiada system komputerowy podłączony do Internetu i wymienia za jego pośrednictwem informacje. Informacje mogą być przekazywane przez połączenie sieci. W konsekwencji to połączenie jest jeszcze bardziej narażone na ryzyko złośliwego oprogramowania ze strony tych, którzy chcą zdobyć poufne informacje, działając od wewnątrz (kopiując informacje, używając złośliwego kodu) lub z zewnątrz.

Aby przeciwdziałać tym zagrożeniom, bezpieczeństwo informacji wymaga opracowania takich pojęć, jak znakowanie danych, szyfrowanie kluczem publicznym (PKI) i wielopoziomowe zabezpieczenia (MLS). Oprócz problemów z łączeniem sieci coraz łatwiej jest przenosić duże ilości informacji (i to w sposób stosunkowo trudny do wykrycia w przypadku włamania), ale także fizycznie przenosić je za pomocą pendrive'ów czy kart pamięci.

Dlatego systemy komputerowe zawierające poufne informacje są coraz częściej projektowane jako środowisko systemu w trybie wysokim, w wielu przypadkach w postaci odizolowanych sieci bez połączenia z innymi sieciami i bez portów USB. Powszechnie akceptowane są trzy kryteria wrażliwości informacji:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

dostępność, integralność i poufność. Zdefiniować można również czwartą cechę nazywaną: Identyfikowalność, Odpowiedzialność, Audytowalność (w odniesieniu do audytów komputerowych) lub Dowód. Stosowane jest również piąte kryterium: niezaprzeczalność, która zapewnia wymianę wiadomości między nadawcą a odbiorcą.

Cyberataki i ramy kompetencji

Zapewnienie bezpieczeństwa informacji jest kluczowe. Systemy kontroli wewnętrznej są ważne, a ich brak bardzo często stanowi zagrożenie dla cyberbezpieczeństwa.
Ochrona informacji i systemów informatycznych obejmuje ochronę przed nieuprawnionym dostępem lub modyfikacją informacji podczas przechowywania, przetwarzania lub przesyłania, a także przed odmową usługi upoważnionym użytkownikom. Bezpieczeństwo informacji obejmuje środki niezbędne do wykrywania, dokumentowania i przeciwdziałania takim zagrożeniom. Bezpieczeństwo informacji składa się z bezpieczeństwa komputerowego i bezpieczeństwa komunikacji(zwane także jako INFOSEC). Obejmuje pojęcia jak: bezpieczeństwo komunikacji; bezpieczeństwo komputera; bezpieczeństwo informacji; System informacyjny.
Kontrole wewnętrzne są stosowane przez kierownictwo, bezpieczeństwo IT, zespoły finansowe, księgowe i operacyjne, aby osiągnąć zapewnienie wiarygodności i dokładności informacji finansowych. Kontrole wewnętrzne zapewniają, że dokładne, aktualne i kompletne informacje znajdują odzwierciedlenie w rachunkowości systemu i raportach finansowych.
Uczestnicy kursu będą informowani o takich aspektach, czytając odpowiedni tekst, oglądając webinaria i rozwiązując ćwiczenia we własnym tempie. Wszystkie te dokumenty znajdują się na cyfrowej interaktywnej platformie projektowej.
Kursanci mogą przetestować swoje odpowiedzi wykonując quizy. Odpowiedzi na inne ćwiczenia należy zapisać na odpowiednim forum dyskusyjnym i przedyskutować z mentorem na wspólnym zorganizowanym spotkaniu raz w tygodniu. Kursant może współpracować z innymi osobami i mentorem, szczególnie podczas spotkań. Będą one wspierane w celu opracowania e-portfolio ważnego dla refleksji i oceny szkolenia.

Treść materiału edukacyjnego

Cyberataki i ramy kompetencji

Ramy kompetencji są regularnie wykorzystywane przez firmy do zrozumienia ich wymagań opartych na umiejętnościach, wymaganych kompetencji, umiejętności pracowników i luk.

Kiedy ramy kompetencji są opracowywane z uwzględnieniem profilu firmy i interesów pracowników, mogą poprawić wydajność i zapewnić jasność dla każdego indywidualnego wymogu roli i rozwijać talenty w miejscu pracy. W ostatnich latach, ze względu na wiele cyberataków, ramy bezpieczeństwa cybernetycznego są przyjmowane głównie przez duże organizacje (firmy, organizacje pozarządowe i inne podmioty) lub przez podmioty państwowe.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Udany cyberatak może spowodować poważne szkody w działalności firmy. Może to wpłynąć na jej wyniki finansowe, a także na status biznesowy firmy i zaufanie konsumentów. Wpływ naruszenia bezpieczeństwa można podzielić na trzy kategorie: finansowe, reputacyjne i prawne.

Cyberataki

Cyberataki często skutkują znacznymi stratami finansowymi wynikającymi z kradzieży informacji korporacyjnych, informacji finansowych (np. danych bankowych lub danych karty płatniczej), pieniędzy, zakłóceń transakcji (np. niemożności dokonania transakcji online), straty biznesu lub z powodu umowy. Firmy, które doznały cyberataku, zazwyczaj wydają pieniądze związane z naprawą systemów, sieci i urządzeń, których dotyczy problem.

Cyberataki mogą zaszkodzić reputacji firmy i zaufaniu klientów do firmy. Może to prowadzić do utraty klientów, spadku sprzedaży i zmniejszenia zysków. Efekt utraty reputacji może nawet wpłynąć na dostawców firmy lub wpłynąć na relacje z partnerami, inwestorami i innymi stronami trzecimi zaangażowanymi w działalność firmy.

Tak więc przepisy dotyczące ochrony danych i prywatności wymagają zarządzania bezpieczeństwem wszystkich danych osobowych przechowywanych przez firmę (jej własnych pracowników lub klientów). Jeśli dane te zostaną przypadkowo lub celowo naruszone, a firma nie wdroży odpowiednich środków bezpieczeństwa, może spotkać się z karami regulacyjnymi.

Ryzyka w firmie

Ważne jest, aby odpowiednio zarządzać ryzykiem. Po wystąpieniu ataku skuteczne narzędzie cyberbezpieczeństwa lub plan reagowania na incydenty, tj. korzystanie z konsultanta cybernetycznego, może pomóc w:

- zmniejszeniu wpływ ataku
- zgłoszeniu incydent właściwemu organowi
- oczyszczeniu systemów, których dotyczy problem
- uruchomieniu działalności swojej firmy w jak najkrótszym czasie.

Konieczne jest inwestowanie w szkolenia i edukację użytkowników w zakresie cyberbezpieczeństwa, aby uniknąć ataków i stale rozwijać świadomość strategii cybernetycznej w swojej organizacji.

Ramy bezpieczeństwa cybernetycznego

Struktura cyberbezpieczeństwa to zestaw najlepszych praktyk i udokumentowanych procesów, które są wykorzystywane do opracowywania zasad bezpieczeństwa IT w organizacji. Jednak w przeciwieństwie do tradycyjnej polityki ściśle związanej z dziedziną prawną, ramy cyberbezpieczeństwa powinny również zawierać udokumentowane przykłady problemów, których należy unikać dzięki tym politykom, oraz odpowiednie procesy i sposoby wdrażania polityki bezpieczeństwa opisanej w tych ramach.

Jest to zarówno przewodnik dla pracowników i użytkowników, jak i atrakcyjne kompendium najlepszych praktyk bezpieczeństwa, z którymi mogą zapoznać się upoważnione strony zewnętrzne (takie jak władze). Ramy kompetencji w zakresie cyberbezpieczeństwa mogą również pomóc

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

w lepszej ocenie kompetencji potrzebnych do uniknięcia ataków, luk i środków zaradczych.

Bezpieczeństwo cybernetyczne

Pomimo zwiększonej świadomości i odważnych wysiłków, znany jest bardzo znaczący i rosnący niedobór specjalistów ds. bezpieczeństwa cybernetycznego w Unii Europejskiej oraz wiedzy i umiejętności pracowników w celu uniknięcia cyberataków na całym świecie, a niedobory te nadal stanowią poważne problemy dla sektora publicznego i prywatnego.

Badanie 2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) szacuje, że na całym świecie jest 2,8 miliona specjalistów ds. Cyberbezpieczeństwa, podczas gdy luka wynosi w rzeczywistości 4,07 miliona.

W badaniu zauważono, że obecna luka w Europie wynosi 291 000, a liczba ta podwoiła się w porównaniu z poprzednimi latami. Wiele krajów o wysoko rozwiniętej wiedzy fachowej woli tworzyć własne przepisy i dokumenty, ale wiele krajów oraz małych i średnich przedsiębiorstw (MŚP) potrzebuje pomocy w tym kontekście.

Inżynieria społeczna

- oznacza manipulowanie ludźmi (często przy użyciu metod psychologicznych) w celu uzyskania dostępu do danych, dokumentów i informacji interesujących atakującego.
- jest obecnie jednym z głównych zagrożeń dla bezpieczeństwa informacji i jest skuteczną formą cyberprzestępczości.
- może mieć niebezpieczne reperkusje, na przykład naruszenia danych, bardziej niż jakikolwiek inny rodzaj ataku.
- ataki mają cel finansowy, a zatem organizacje straciły znaczne kwoty pieniędzy.
- jest to szczególnie niebezpieczne, ponieważ opiera się bardziej na błędzie ludzkim niż na lukach w oprogramowaniu i systemach operacyjnych.

Firmy:

- mogą cierpieć z powodu utraty produktywności, spadku morale pracowników i trudności w powrocie do pełnej funkcjonalności.
- mają szkody dla reputacji, ponieważ klienci nie są przekonani, że organizacja może się chronić.
- często uruchomiają starą reakcję na incydent.
- powinny zapewniać oprogramowanie zabezpieczające, które pomaga zapobiegać przyszłym atakom.
- często muszą przekwalifikować pracowników, aby byli gotowi na ataki.

Inżynieria społeczna; Szkolenia (świadomość cybernetyczna)

- pracowników i menedżerów, dla których ważne jest rozpoznanie ataków socjotechnicznych, ponieważ ryzyko stania się ofiarą jest wysokie.
- mogą być włączone do społecznych, indywidualnych i obywatelskich programów świadomości bezpieczeństwa oraz chronić osoby i ich organizacje.
- szczególnie brakuje w MŚP, które mają mniej zasobów, dlatego należy im pomóc w poważnym

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

potraktowaniu szkoleń w zakresie świadomości cybernetycznej i zapewnieniu pracownikom możliwości ich wykorzystania.

Szkolenia i mentoring

Przedsiębiorcy, także przyszli, potrzebują złożonych sposobów myślenia oraz umiejętności rozumienia i integrowania wiedzy z różnych sektorów, co wymaga interdyscyplinarnego uczenia się. Złożone problemy inżynierskie wymagają stworzenia interdyscyplinarnej sytuacji w niemal naturalny sposób.

W podejściu interdyscyplinarnym uczniowie powinni integrować informacje z różnych dyscyplin i dziedzin. Rozwijają interdyscyplinarne zrozumienie, uczą się integrować obszary wiedzy i specyficzne dla dyscypliny sposoby myślenia.

Zwiększa to umiejętności poznawcze i krytyczne myślenie bardziej niż za pomocą pojedynczych środków dyscyplinarnych.

Umiejętności w zakresie przedsiębiorczości i mentoring

Ocena wyników osób uczących się w rozwijaniu umiejętności w zakresie przedsiębiorczości może przyjąć całościowe spojrzenie, w tym spojrzenie na środowisko uczenia się i efekty uczenia się, oraz ułatwić interaktywne, skuteczne i aktywne uczenie się.

Mentoring jest doświadczoną metodą wspierania bardziej indywidualnego uczenia się oraz zdobywania umiejętności osobistych i zawodowych dla nowych zawodów. Istnieją badania nad wynikami mentoringu, ale niewiele jest badań na temat samego mentoringu.

Mentoring oferuje szereg korzyści dla pracowników, którzy szkolą się w firmach. Interdyscyplinarny mentoring zespołowy zyskał na znaczeniu w ostatnich latach, odzwierciedlając potrzebę zmiany orientacji mentoringu, ponieważ różne zmiany i dziedziny przedsiębiorczości są coraz bardziej multidyscyplinarne.

Interdyscyplinarny mentoring i sieci mentorów mogą tworzyć synergię w grupach, generować innowacyjne pomysły i złożone rozwiązania wyzwań oraz tworzyć możliwości współpracy i pracy.

Pojęcia, definicje i terminy

Termin "**cyberprzestrzeń**" został przedstawiony w 1982 roku przez Williama Gibsona. Termin ten wszedł do codziennego życia w 1990 roku wraz z pojawieniem się World Wide Web.

infrastruktura cybernetyczna – infrastruktura technologii informacyjno-komunikacyjnych, składająca się z systemów informatycznych, powiązanych aplikacji, sieci i usług łączności elektronicznej;

cyberprzestrzeń – środowisko wirtualne, generowane przez infrastrukturę cybernetyczną, w tym treści informacyjne przetwarzane, przechowywane lub przesyłane, a także działania wykonywane w nim przez użytkowników;

cyberbezpieczeństwo - stan normalności wynikający z zastosowania zestawu proaktywnych

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

i reaktywnych środków, które zapewniają poufność, integralność, dostępność, autentyczność i niezaprzeczalność informacji w formacie elektronicznym, publicznych lub prywatnych zasobów i usług w cyberprzestrzeni.

Proaktywne i reaktywne środki mogą obejmować polityki bezpieczeństwa, koncepcje, standardy i wytyczne, zarządzanie ryzykiem, szkolenia i działania uświadamiające, wdrażanie rozwiązań technicznych w celu ochrony infrastruktury cybernetycznej, zarządzanie tożsamością, zarządzanie konsekwencjami;

cyberobrona – działania prowadzone w cyberprzestrzeni w celu ochrony, monitorowania, analizowania, wykrywania, przeciwdziałania agresji oraz zapewnienia terminowej reakcji na zagrożenia dla infrastruktury cybernetycznej specyficznej dla obrony narodowej;

operacje w sieciach komputerowych - złożony proces planowania, koordynacji, synchronizacji, harmonizacji i przeprowadzania działań w cyberprzestrzeni w celu ochrony, kontroli i wykorzystania sieci komputerowych w celu uzyskania przewagi informacyjnej, jednocześnie z neutralizacją możliwości przeciwnika;

zagrożenie cybernetyczne - okoliczność lub zdarzenie, które stanowi potencjalne zagrożenie dla bezpieczeństwa cybernetycznego;

cyberatak - wrogie działania przeprowadzane w cyberprzestrzeni, które mogą mieć wpływ na bezpieczeństwo cybernetyczne;

incydent cybernetyczny - zdarzenie zachodzące w cyberprzestrzeni, którego konsekwencje wpływają na bezpieczeństwo cybernetyczne;

cyberterroryzm - działania z premedytacją prowadzone w cyberprzestrzeni przez politycznie, ideologicznie lub religijnie motywowane osoby, grupy lub organizacje, które mogą spowodować materialne zniszczenie lub ofiary, mogące wywołać panikę lub terror;

cyberszpiegostwo - działania prowadzone w cyberprzestrzeni, mające na celu uzyskanie nieuprawnionych informacji poufnych w interesie podmiotu państwowego lub niepaństwowego;

przestępczość komputerowa - wszystkie czyny przewidziane w prawie karnym lub innych specjalnych przepisach, które stanowią zagrożenie społeczne i są popełniane z winą, za pośrednictwem lub na infrastrukturze cybernetycznej;

podatność na zagrożenia w cyberprzestrzeni - słabość w projektowaniu i wdrażaniu infrastruktury cybernetycznej lub powiązanych środków bezpieczeństwa, które mogą zostać wykorzystane przez zagrożenie;

ryzyko bezpieczeństwa w cyberprzestrzeni - prawdopodobieństwo, że zagrożenie się zmaterializuje, wykorzystując określoną podatność specyficzną dla infrastruktury cybernetycznej;

zarządzanie ryzykiem - złożony, ciągły i elastyczny proces identyfikacji, oceny i przeciwdziałania zagrożeniom bezpieczeństwa cybernetycznego, oparty na wykorzystaniu złożonych technik

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

i narzędzi, w celu zapobiegania wszelkiego rodzaju stratom;

zarządzanie tożsamością - metody walidacji tożsamości osób, gdy uzyskują dostęp do określonych infrastruktur cybernetycznych.

Elementy kontroli wewnętrznej

Zgodnie ze standardem INTOSAI GOV 9100 "Wytyczne dotyczące standardów kontroli wewnętrznej". W 2001 r. na Kongresie Międzynarodowej Organizacji Najwyższych Organów Kontroli (INCOSAI) podjęto decyzję o aktualizacji wytycznych INTOSAI dotyczących standardów kontroli wewnętrznej w sektorze publicznym, pierwotnie wydanych w 1992 r., poprzez wprowadzenie do dokumentu wszystkich aspektów ostatnich zmian w dziedzinie kontroli wewnętrznej oraz zintegrowanie szeregu elementów modelu COSO (Kontrola wewnętrzna – zintegrowane ramy).

Poprzez włączenie go do Wytycznych - działania prowadzonego przez grupę operacyjną Komitetu Standardów Kontroli Wewnętrznej INTOSAI - podjęto próbę uzyskania jednolitego zrozumienia funkcjonowania nowego systemu kontroli wewnętrznej przez przedstawicieli Najwyższych Organów Kontroli.

"Wytyczne INTOSAI dotyczące standardów kontroli wewnętrznej w sektorze publicznym" należą do kategorii INTOSAI GOV (wytyczne dotyczące dobrego zarządzania) i są uważane za niezwykle przydatne zarówno dla menedżerów sektora publicznego, którzy muszą wdrożyć system kontroli wewnętrznej, jak i zewnętrznych audytorów publicznych, którzy muszą znać ten system i go oceniać.

Standardy kontroli wewnętrznej

Zgodnie z wytycznymi INTOSAI GOV 9100) kontrola wewnętrzna składa się z pięciu współzależnych komponentów (identycznych z tymi z modelu COSO):

- Środowisko sterowania
- Ocena ryzyka
- Działania kontrolne
- Informacja i komunikacja
- Monitoring

Kontrola wewnętrzna ma na celu zapewnienie wystarczającej pewności co do osiągnięcia ogólnych celów instytucji. Cele jasno określone przez szefów podmiotu oraz odpowiednie zaplanowanie budżetu są obowiązkowym warunkiem skutecznej kontroli wewnętrznej.

Środowisko kontroli

Środowisko kontroli obejmuje ogólną postawę, świadomość i działania podejmowane przez kierownictwo i osoby odpowiedzialne za zarządzanie w odniesieniu do systemu kontroli wewnętrznej i jego znaczenia w jednostce. Środowisko kontroli nadaje ton organizacji, wpływając na świadomość kontroli na poziomie

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

personelu.

Stanowi podstawę wszystkich innych elementów kontroli wewnętrznej, zapewniając dyscyplinę w organizacji, która musi być przestrzegana i strukturę podmiotu, aby system kontroli wewnętrznej mógł być skutecznie stosowany. Środowisko kontroli wewnętrznej jest skutecznym narzędziem zapobiegania korupcji i nadużyciom finansowym.

Elementy definiujące środowisko sterowania to:

- uczciwość osobista i zawodowa, wartości etyczne ustanowione przez kierownictwo dla wszystkich pracowników, w tym stałe wspierające podejście do kontroli wewnętrznej;
- ciągła troska o zarządzanie kompetencjami personelu;
- "ton nadany z góry" (filozofia i styl zarządzania działalnością);
- struktura organizacyjna podmiotu;
- polityka i praktyki HR.

Rodzaje kontroli bezpieczeństwa cybernetycznego

Kontrola cyberbezpieczeństwa to mechanizmy stosowane do zapobiegania, wykrywania i łagodzenia zagrożeń i ataków cybernetycznych. Mechanizmy obejmują zarówno fizyczne kontrole, takie jak ochroniarze i kamery monitorujące, jak i kontrole techniczne, w tym zapory ogniowe i uwierzytelnianie wieloskładnikowe.

Jednostronne podejście do cyberbezpieczeństwa jest po prostu przestarzałe i nieskuteczne. Ponieważ niemożliwe jest zapobieżenie wszystkim atakom w dzisiejszym krajobrazie zagrożeń, organizacje powinny ocenić swoje zasoby w oparciu o ich znaczenie dla firmy i odpowiednio ustanowić kontrole.

Dodatkowym wyzwaniem jest to, że pracownicy prawdopodobnie nie będą przestrzegać zasad zgodności, jeśli rygorystyczne kontrole zostaną wdrożone we wszystkich aktywach firmy. Ważność kontrolki powinna bezpośrednio odzwierciedlać krajobraz zasobów i zagrożeń.

Konsekwencje ujawnienia przez hakera tysięcy danych osobowych klientów za pośrednictwem bazy danych w chmurze mogą być znacznie większe niż w przypadku naruszenia bezpieczeństwa laptopa pracownika.

Kontrola bezpieczeństwa cybernetycznego

"Istnieje wiele różnych sposobów stosowania kontroli w oparciu o naturę tego, co próbujesz chronić" - powiedział Joseph MacMillan, autor Infosec Strategies and Best Practices and cybersecurity global black belt w Microsoft.

"Jaka jest natura zagrożenia, przed którym próbujesz się chronić?

Czy to złośliwy aktor?

A może jest to niszczycielski atak?"

Zabezpieczanie zasobów informacyjnych

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Odnosi się do wdrożenia odpowiednich środków kontroli bezpieczeństwa informacji w odniesieniu do aktywów. Chcemy mieć pewność, że skupiamy się na silnych i skutecznych ideologiach, aby zrozumieć wybór odpowiednich kontroli, co oznacza, że zasób jest uważany za "wystarczająco bezpieczny" w oparciu o jego krytyczność i klasyfikację. Istnieją różne klasy, które dzielą typy kontroli:

- Kontrole administracyjne/zarządcze to zasady i procedury firmy. Nie są tak "fajne" jak nowa kontrola oprogramowania, ale istnieją, aby zapewnić strukturę i wskazówki osobom i innym członkom organizacji, zapewniając, że nikt nie zostanie ukarany grzywną lub nie spowoduje naruszenia.
- Fizyczne elementy sterujące, które ograniczają dostęp do systemów w sposób fizyczny.
- Kontrole techniczne / logiczne to te, które ograniczają dostęp w oparciu o sprzęt lub oprogramowanie, takie jak szyfrowanie, czytniki linii papilarnych, uwierzytelnianie lub moduły zaufanej platformy (TPM).

Nie ograniczają one dostępu do systemów fizycznych, tak jak robią to fizyczne kontrole, ale raczej dostęp do danych lub treści. Kontrole operacyjne to takie, które obejmują ludzi przeprowadzających procesy na co dzień. Przykłady mogą obejmować szkolenia uświadamiające, klasyfikację zasobów i przegląd plików dziennika.

Rodzaje elementów sterujących

Istnieją mechanizmy kontroli zapobiegawczych, które zapobiegają działaniu i obejmują zapory, ogrodzenia i uprawnienia dostępu.

Polecenia detektywistyczne są wyzwalane tylko w trakcie lub po zdarzeniu, takim jak nadzór wideo lub systemy wykrywania włamań. Środki odstraszające zniechęcają zagrożenia przed próbą wykorzystania luki w zabezpieczeniach, takiej jak "Watchdog" lub znak obecności psów. Kontrole korekcyjne są w stanie podejmować działania z jednego stanu do drugiego. Tutaj omówiono polecenia fail open i fail closed.

Polecenia odzyskiwania odzyskują coś z utraty, na przykład odzyskiwanie dysku twardego. Kontrole kompensacyjne to te, które próbują zrekompensować braki w innych kontrolach, takich jak regularne przeglądanie dzienników dostępu. Ten przykład jest również kontrolą detektywistyczną, ale kontrole wynagrodzeń mogą być różnego rodzaju.

Kolejność kontroli

Zniechęca aktorów do prób uzyskania dostępu do czegoś, czym nie powinni być. Odmów/Zablokuj dostęp za pomocą kontroli prewencyjnej, takiej jak uprawnienia dostępu lub uwierzytelnianie.

Wykryj ryzyko, rejestrując wykrywanie, na przykład za pomocą oprogramowania do ochrony punktów końcowych. Opóźnij proces przed ponownym powtórzeniem ryzyka, na przykład za pomocą funkcji "zbyt wiele prób" wprowadzenia hasła.

Popraw sytuację, reagując na kompromis, na przykład plan reagowania na incydenty. Odzyskiwanie z zagrożonego stanu, takiego jak generator kopii zapasowych, który przywraca dostępność serwera.

Ponadto w zakresie ciągłego doskonalenia powinniśmy monitorować wartość każdego aktywa pod kątem

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

ewentualnych zmian. Powodem jest to, że być może będziemy musieli ponownie przemyśleć nasze mechanizmy kontroli w celu ochrony tych zasobów, jeśli z czasem staną się one mniej lub bardziej wartościowe lub podczas niektórych ważnych wydarzeń w organizacji.

Kontrola i odzyskiwanie

Kiedy patrzymy na kontrole, powinniśmy również myśleć o przywróceniu, chcemy być w stanie odzyskać poprawny stan po wszelkich niekorzystnych sytuacjach lub zmianach w aktywach i ich wartości. Jako przykłady mówimy o kopiach zapasowych, redundancji, procesach przywracania i tym podobnych.

Koncepcją do zapamiętania, szczególnie w dobie chmury, SaaS, PaaS, IaaS, rozwiązań innych firm i wszelkich innych form "cudzego komputera", jest zapewnienie, że umowy o gwarantowanym poziomie usług (SLA) są jasno zdefiniowane i mają maksymalne dopuszczalne umowy przestojów, a także kary za nieprzestrzeganie tych umów. Jest to przykład kontroli kompensacyjnej.

Pytania:

Forum dyskusyjne, na które należy odpowiedzieć krótkim wyjaśnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentoringowych

1. Jakie są zagrożenia w przedsiębiorstwie związane z cyberatakami?
2. Nazwij niektóre rodzaje kontroli cyberbezpieczeństwa.
3. Jakie są standardy kontroli wewnętrznej.
4. Jak kontrolować i odzyskiwać informacje.

Pytania samooceny. Po udzieleniu odpowiedzi uczeń może zobaczyć wyniki i porównać je z tymi zapisanymi na platformie

- Ryzyko cyberataków w firmie.
- Standardy kontroli wewnętrznej i role.
- Środowisko sterowania.

Załączniki

Prezentacja PowerPoint

Filmy video

Odnośniki:

- Cyber Attacks on Companies: Are You at Risk?
- The rising strategic risks of cyberattacks

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- 10 Common Cyber Security Risks For Businesses
- Internal Controls and Data Security: How to Develop Controls That Meet Your IT Security Needs
- Internal Controls Over Information Systems

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.