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

Moduł szkoleniowy InCyT

Bezpieczeństwo informacji dla menedżerów Część 2, Tydzień 3 Moduł: Zarządzanie bezpieczeństwem informacji -1	
Zajęcia edukacyjne	❑ **Webinar** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacje** ❑ **Inne**
Odpowiedzialni za zajęcia	• Fatma Gökdemir • Ali Gökdemir
Cele aktywności edukacyjnej	1. Bezpieczeństwo informacji 2. Polityka bezpieczeństwa informacji 3. Role w zakresie bezpieczeństwa informacji
Umiejętności do zdobycia	• IS 1 • IS 3 • MS 3
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest potrzebne?***
	• Średniozaawansowane umiejętności obsługi komputera

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

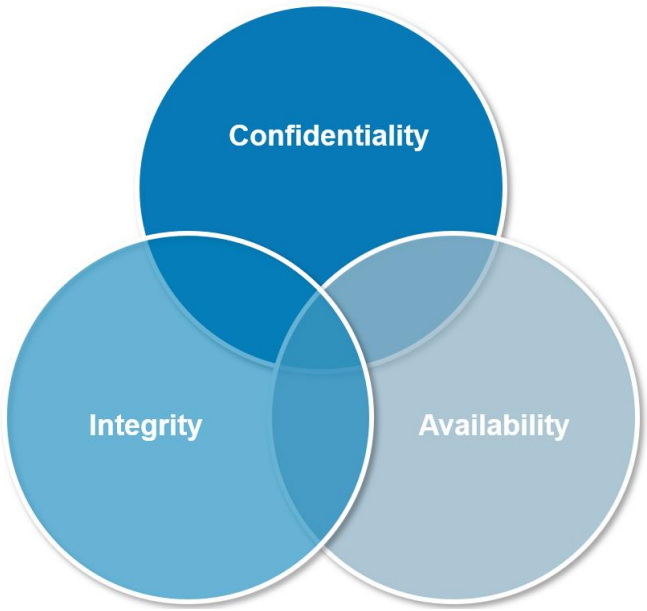
Krótka informacja o module

Opis
Bezpieczeństwo informacji ma ogromne znaczenie w zapewnieniu ciągłości działania każdej organizacji i zapewnia ochronę krytycznych informacji organizacji i innych zasobów informacyjnych w różnych środowiskach, zwłaszcza elektronicznych. Nie tylko duże firmy, holdingi, ale także MŚP, agencje rządowe, każda organizacja non-profit, szkoła lub osoby same w sobie stale doświadczają problemów i zagrożeń związanych z bezpieczeństwem informacji, choć na różnych poziomach. W inwestycjach wychodzących naprzeciw tym zagrożeniom najdroższe i najbardziej złożone rozwiązanie nie zawsze jest najbezpieczniejszym rozwiązaniem. Każda osoba lub organizacja musi wybrać i wdrożyć najbardziej odpowiednie i poprawne rozwiązanie. Nie należy zapominać, że o ile proste i tanie rozwiązanie bezpieczeństwa może być niewystarczające dla niektórych instytucji, o tyle to samo rozwiązanie może być wystarczające i skuteczne dla innej instytucji. Jednak bezpieczeństwo informacji nie jest pracą, którą należy rozpocząć i zakończyć. Zarządzanie bezpieczeństwem informacji to cykl życia, który musi być stale zarządzany i kontrolowany tak długo, jak długo istnieją instytucje i informacje. W tym module wyjaśniona zostanie koncepcja bezpieczeństwa informacji, jej znaczenie i to, co należy zrobić dla bezpieczeństwa informacji. Temat został poparty praktycznym przykładem

Treść materiału edukacyjnego

1. Bezpieczeństwo informacji

Bezpieczeństwo informacji ma na celu zapobieganie nieautoryzowanemu dostępowi, wykorzystaniu, modyfikacji, ujawnieniu, zniszczeniu, wymianie i uszkodzeniu informacji. Składa się z trzech podstawowych elementów zwanych poufnością, integralnością i dostępnością (rysunek 1). Jeśli którykolwiek z tych trzech podstawowych elementów zabezpieczeń zostanie uszkodzony, wystąpi luka w zabezpieczeniach.



Rys. 1. Elementy bezpieczeństwa informacji

- Poufność: Jest to ochrona informacji przed nieautoryzowanym dostępem.
- Integralność: Informacje nie są zmieniane przez osoby nieupoważnione.
- Dostępność: Informacje są dostępne i użyteczne w razie potrzeby przez upoważnione osoby.

1.1. Co to jest polityka bezpieczeństwa informacji?

Zagrożenia bezpieczeństwa stale ewoluują, a wymagania dotyczące zgodności stają się coraz bardziej złożone. Organizacje muszą stworzyć kompleksową politykę bezpieczeństwa informacji, aby uwzględnić oba wyzwania. Polityka bezpieczeństwa informacji (ISP) to zestaw reguł, zasad i procedur zaprojektowanych w celu zapewnienia, że wszyscy użytkownicy końcowi i sieci w organizacji spełniają minimalne wymagania dotyczące bezpieczeństwa IT i ochrony danych. Polityka bezpieczeństwa informacji umożliwia koordynowanie i egzekwowanie programu bezpieczeństwa oraz informowanie o środkach bezpieczeństwa stron trzecich i audytorów zewnętrznych.

1.2. Jaki jest cel polityki bezpieczeństwa informacji?

Polityka bezpieczeństwa informacji ma na celu wprowadzenie zabezpieczeń i ograniczenie dystrybucji danych tylko do osób z autoryzowanym dostępem. Organizacje tworzą ISP, aby:

- Ustanowić ogólne podejście do bezpieczeństwa informacji

- Dokumentować środki bezpieczeństwa i polityki kontroli dostępu użytkowników
- Wykrywać i minimalizować wpływ zagrożonych aktywów informacyjnych, takich jak niewłaściwe wykorzystanie danych, sieci, urządzeń mobilnych, komputerów i aplikacji
- Chronić reputację organizacji
- Pracować zgodnie z wymogami prawnymi i regulacyjnymi, takimi jak ENISA, NIST, GDPR, HIPAA i FERPA
- Chronić dane swoich klientów, takie jak numery kart kredytowych
- Zapewnić skuteczne mechanizmy reagowania na skargi i zapytania związane z rzeczywistymi lub postrzeganymi zagrożeniami dla cyberbezpieczeństwa, takimi jak phishing, złośliwe oprogramowanie i ransomware
- Ograniczyć dostęp do kluczowych zasobów informatycznych do osób, które mają dopuszczalny dostęp

1.3. Dlaczego polityka bezpieczeństwa informacji jest ważna?

Stworzenie skutecznej polityki bezpieczeństwa informacji, która spełnia wszystkie wymagania dotyczące zgodności, jest kluczowym krokiem w zapobieganiu incydentom bezpieczeństwa, takim jak wycieki danych i naruszenia danych.

ISP są ważni dla nowych i uznanych organizacji. Rosnąca cyfryzacja oznacza, że każdy pracownik generuje dane, a część tych danych musi być chroniona przed nieautoryzowanym dostępem. W zależności od branży może być nawet chroniony przez przepisy ustawowe i wykonawcze.

Dane wrażliwe, dane osobowe (PII) i własność intelektualna muszą być chronione w wyższym standardzie niż inne dane.

Czy Ci się to podoba, czy nie, bezpieczeństwo informacji (InfoSec) jest ważne na każdym poziomie Organizacji. I poza organizacją.

Zasady bezpieczeństwa informacji mogą mieć następujące zalety dla organizacji:

- **Ułatwia integralność, dostępność i poufność danych —** szczegółowe zasady bezpieczeństwa informacji standaryzują reguły i procesy, które chronią przed wektorami zagrażającymi integralności, dostępności i poufności danych.
- **Chroni wrażliwe dane —** w polityce bezpieczeństwa informacji priorytetowo traktuje się ochronę własności intelektualnej i danych wrażliwych, takich jak dane osobowe (PII).
- **Minimalizuje ryzyko incydentów związanych z bezpieczeństwem** — Polityka bezpieczeństwa informacji pomaga organizacjom zdefiniować procedury identyfikacji i

łagodzenia luk w zabezpieczeniach i zagrożeń. Zawiera również szczegółowe informacje na temat szybkich reakcji, aby zminimalizować szkody podczas incydentu bezpieczeństwa.

- **Wykonuje programy bezpieczeństwa w całej organizacji** — zasady bezpieczeństwa informacji zapewniają ramy dla operacjonalizacji procedur.
- **Zapewnia jasne oświadczenie o zabezpieczeniach dla stron trzecich** — zasady bezpieczeństwa informacji podsumowują stan zabezpieczeń organizacji i wyjaśniają, w jaki sposób organizacja chroni zasoby i zasoby IT. Ułatwiają szybkie reagowanie na prośby stron trzecich o informacje od klientów, partnerów i audytorów.
- **Pomaga zachować zgodność z wymogami prawnymi** — utworzenie polityki bezpieczeństwa informacji może pomóc organizacjom zidentyfikować luki w zabezpieczeniach związane z wymogami prawnymi i rozwiązać je.

1.4. Co powinno znaleźć się w polityce bezpieczeństwa informacji?

Polityka bezpieczeństwa informacji może być trudna do zbudowania od zera; musi być solidna i zabezpieczać Twoją organizację od wszystkich stron. Powinna obejmować całe oprogramowanie, sprzęt, parametry fizyczne, zasoby ludzkie, informacje i kontrolę dostępu. Musi być również elastyczna i mieć miejsce na przegląd i aktualizację, a co najważniejsze, musi być praktyczna i egzekwowalna. Myślenie życzeniowe nie pomoże Ci, gdy opracowujesz politykę bezpieczeństwa informacji. Musisz współpracować z głównymi interesariuszami, aby opracować politykę, która działa dla Twojej firmy i pracowników, którzy będą odpowiedzialni za realizację polityki.

1. ***Zasady dopuszczalnego użytkowania***

Zasady te określają dopuszczalne korzystanie ze sprzętu komputerowego i Internetu w organizacji. Niewłaściwe korzystanie z Internetu lub komputerów otwiera Twoją firmę na ryzyko, takie jak ataki wirusów, zainfekowane systemy sieciowe i usługi oraz kwestie prawne, dlatego ważne jest, aby mieć na piśmie to, co jest, a co nie jest dopuszczalne.

Zasady dopuszczalnego użytkowania powinny określać, za co pracownicy są odpowiedzialni w odniesieniu do ochrony sprzętu firmy, na przykład zamykania komputerów, gdy są z dala od biurka lub zabezpieczania tabletów lub innych urządzeń elektronicznych, które mogą zawierać poufne informacje. Powinien również określać, jakie są prawa firmy i jakie działania nie są zabronione na sprzęcie i sieci firmy.

2. ***Polityka „czystego biurka”***

Polityka czystego biurka koncentruje się na ochronie zasobów fizycznych i informacji. Idealnie byłoby, gdyby ta polityka zapewniła, że wszystkie wrażliwe i poufne materiały zostaną zablokowane lub w inny sposób zabezpieczone, gdy nie będą używane lub pracownik opuści biurko. Zasady te powinny określać minimalne wymagania dotyczące utrzymywania czystego biurka, na przykład w przypadku gdy poufne informacje o pracownikach, własności intelektualnej,

klientach i dostawcach mogą być przechowywane i dostępne. Powinien również obejmować takie rzeczy, jak rodzaje materiałów, które należy zniszczyć lub wyrzucić, czy hasła muszą być używane do pobierania dokumentów z drukarki oraz jakie informacje lub mienie muszą być zabezpieczone fizycznym zamkiem. Oprócz tego, że jest to powszechna i ważna część każdej polityki bezpieczeństwa informacji, polityka czystego biurka jest zgodna z ISO 27001/17799 i pomoże Twojej firmie przejść audyt certyfikacyjny.

3. ***Polityka reagowania na naruszenia danych***

Jest to również znane jako plan reagowania na incydenty. Celem polityki reagowania na naruszenie danych jest ustalenie celów i wizji tego, jak Twoja organizacja zareaguje na naruszenie danych. Ten plan pomoże zmniejszyć ryzyko bycia ofiarą cyberataku, ponieważ szczegółowo określi, w jaki sposób organizacja planuje chronić zasoby danych w całym procesie reagowania na incydenty.

Polityka ta powinna określać, kogo dotyczy i kiedy wchodzi w życie, w tym definicję naruszenia, role i obowiązki personelu, standardy i wskaźniki, mechanizmy raportowania, korygowania i informacji zwrotnej.

4. ***Zasady planu odzyskiwania po awarii***

Ta polityka różni się od planu reagowania na naruszenie danych, ponieważ jest to ogólny plan awaryjny dotyczący tego, co należy zrobić w przypadku katastrofy lub jakiegokolwiek zdarzenia, które powoduje przedłużone opóźnienie usługi. Zasady te powinny opisywać proces odzyskiwania systemów, aplikacji i danych podczas lub po wystąpieniu wszelkiego rodzaju awarii powodujących poważną awarię. Ten plan odzyskiwania po awarii powinien być aktualizowany co roku.

Plan awaryjny powinien obejmować następujące elementy:

- Plan pomocy w nagłych wypadkach. Wyraźnie wymień, z kim należy się skontaktować, kiedy należy się z nimi skontaktować i jak się z nimi skontaktujesz?
- Plan sukcesji. Opisz przepływ odpowiedzialności, gdy normalny personel jest niedostępny do wykonywania swoich obowiązków.
- Plan klasyfikacji danych. Wyszczególnij wszystkie dane przechowywane we wszystkich systemach, ich krytyczność i poufność.
- Krytyczność listy usług. Wymień wszystkie świadczone usługi i ich kolejność ważności.
- Plan tworzenia kopii zapasowych i przywracania danych. Szczegółowe informacje o tym, które dane są archiwizowane, gdzie i jak często. Wyjaśnij również, w jaki sposób można odzyskać dane.
- Plan wymiany sprzętu. Należy opisać, które usługi infrastrukturalne są niezbędne do wznowienia świadczenia usług na rzecz klientów.
- Komunikacja publiczna. Dokumentuj, kto będzie właścicielem zewnętrznej funkcji PR i

podaj wytyczne dotyczące tego, jakie informacje mogą i powinny być udostępniane.

- Ważne jest, aby zespół zarządzający przeznaczył czas na przetestowanie planu odzyskiwania po awarii. Podczas tych testów, znanych również jako ćwiczenia na stole, celem jest zidentyfikowanie problemów, które mogą nie być oczywiste w fazie planowania, które mogą spowodować niepowodzenie planu. W ten sposób zespół może dostosować plan, zanim dojdzie do katastrofy.

5. Zasady dotyczące poczty e-mail

Poczta e-mail jest krytycznym kanałem komunikacji dla firm wszystkich rodzajów, a niewłaściwe użycie poczty e-mail może stanowić wiele zagrożeń dla bezpieczeństwa Twojej firmy, niezależnie od tego, czy pracownicy używają poczty e-mail do rozpowszechniania poufnych informacji, czy nieumyślnie narażają sieć na wirusa. Ważne jest, aby wszyscy pracownicy, kontrahenci i agenci działający w imieniu Twojej firmy rozumieli właściwe korzystanie z poczty e-mail oraz mieli określone zasady i procedury archiwizacji, oznaczania i przeglądania wiadomości e-mail w razie potrzeby.

Ta polityka musi określać właściwe wykorzystanie firmowych adresów e-mail i obejmować takie rzeczy, jakie rodzaje komunikacji są zabronione, standardy bezpieczeństwa danych dla załączników, zasady dotyczące przechowywania wiadomości e-mail oraz to, czy firma monitoruje wiadomości e-mail. Polityka ta powinna być również jasno określona dla Twoich pracowników, aby zrozumieli swoją odpowiedzialność za korzystanie z ich adresów e-mail oraz odpowiedzialność firmy za zapewnienie prawidłowego korzystania z wiadomości e-mail. Ta polityka poczty e-mail nie polega na tworzeniu zasady "mam Cię", aby złapać pracowników na niewłaściwym użyciu poczty e-mail, ale aby uniknąć sytuacji, w której pracownicy nadużywają wiadomości e-mail, ponieważ nie rozumieją, co jest, a co nie jest dozwolone.

6. Zasady ochrony klucza szyfrowania użytkownika końcowego

Niektóre dokumenty i komunikaty wewnątrz firmy lub rozpowszechniane wśród użytkowników końcowych mogą wymagać zaszyfrowania ze względów bezpieczeństwa. Przygotuj zasady ochrony tych kluczy szyfrowania, aby nie były ujawniane ani nieuczciwie używane.

Polityka ta powinna określać wszystkie wymagania dotyczące ochrony kluczy szyfrowania i wymieniać konkretne kontrole operacyjne i techniczne stosowane w celu zapewnienia ich bezpieczeństwa. Obejmuje to takie rzeczy, jak sprzęt odporny na manipulacje, procedury tworzenia kopii zapasowych i co zrobić w przypadku zgubienia, kradzieży lub nieuczciwego użycia klucza szyfrowania.

7. Polityka ochrony hasłem

Twoi pracownicy prawdopodobnie mają niezliczone hasła, które muszą śledzić i używać na co

dzień, a Twoja firma powinna mieć jasne, wyraźne standardy tworzenia silnych haseł do swoich komputerów, kont e-mail, urządzeń elektronicznych i wszelkich punktów dostępu do Twoich danych lub sieci.

Ta zasada musi również określać, co pracownicy mogą, a czego nie mogą robić ze swoimi hasłami. Może wydawać się oczywiste, że nie powinni umieszczać swoich haseł w wiadomości e-mail ani udostępniać ich współpracownikom, ale nie należy zakładać, że jest to powszechna wiedza dla wszystkich. Daj swoim pracownikom wszystkie informacje potrzebne do tworzenia silnych haseł i zapewnij im bezpieczeństwo, aby zminimalizować ryzyko naruszenia danych.

Wreszcie, ta zasada powinna określać, co programiści i personel IT muszą zrobić, aby upewnić się, że wszelkie aplikacje lub witryny internetowe uruchamiane przez Twoją firmę przestrzegają środków ostrożności w celu zapewnienia bezpieczeństwa haseł użytkowników.

Badania przeprowadzone w ostatniej dekadzie na całym świecie pokazują, że najbardziej preferowane hasła użytkowników to:

- 123456
- password
- Qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Pomimo corocznych ostrzeżeń lista ta niewiele się zmieniła. W tym celu zaleca się użytkownikom przestrzeganie zestawu reguł ustawiania haseł. Zasady te są wymienione poniżej:

- Ustawianie wymagań dotyczących złożoności, takich jak spełnienie minimalnego wymogu dotyczącego znaków
- Nie wybieranie wcześniej używanych haseł
- Okresowa i być może częsta zmiana haseł
- Używane hasła nie powinny być wybierane z popularnych i słabo używanych haseł, jak na powyższej liście

National Institute of Standards and Technology (NIST) miał na celu rozwiązanie problemu polityki haseł w celu określenia haseł i osiągnięcia określonych standardów. NIST określa szczegóły dotyczące haseł oraz sposobu zarządzania nimi i ich przechowywania. W związku z tym ewentualne hasła należy porównać z listą powszechnie używanych i znanych wartości. Zagadnienia dotyczące określania haseł są następujące:

- Hasła dostarczone przez użytkownika powinny składać się z co najmniej

ośmiu znaków alfanumerycznych.

- Nie powinny to być hasła uzyskane z poprzednich naruszeń.
- Nie powinno być słów słownikowych.
- Nie powinno być dat między 1900-2020, takich jak daty urodzenia.
- Brak powtarzających się lub sekwencyjnych znaków (np. aaaaaaaa lub 1234abcd)
- Słowa specyficzne dla zamierzonego zastosowania, takie jak nazwa usługi, nazwa użytkownika i pochodne nie powinny być w nim zawarte.

Powyższe kryteria należy wziąć pod uwagę przy określaniu haseł i należy tworzyć hasła o złożonych strukturach.

Złożoność hasła : Złożoność hasła jest definiowana jako liczba haseł, które są silne dla hasła, mamy na myśli, że spełnia ono zestaw reguł. Klucz do złożoności hasła zasady są następujące:

- Hasło nie może zawierać nazwy konta ani odmian nazwy konta.
- Hasło musi zawierać zarówno wielkie litery (A-Z), jak i małe litery (a-z).
- Znaki specjalne **(~! @ # $% ^ & * _- + = '| \ () {} [] :;" '<>,.? /)** (Są to znaki, które zwykle pojawiają się wraz z ALT. Jednak waluta, taka jak symbole euro, nie liczy się jako znaki specjalne).
- Należy przestrzegać minimalnej liczby znaków. Ta wartość różni się w zależności od systemu, od użytkownika do użytkownika może ulec zmianie.

Minimalna długość hasła powinna wynosić 8 znaków, a zalecana 12 znaków.
Gdy hasła są tworzone z co najmniej 8 znakami zgodnie z zasadami wymienionymi powyżej, oznacza to co najmniej 218,340,105,584,896 różnych możliwości dla jednego hasła. Prawdopodobieństwo wygenerowanego hasła sprawia, że atak siłowy jest bardzo trudny, ale hasło nadal nie jest niemożliwe do złamania. W przypadku hasła, które jest prawie niemożliwe do złamania, konieczne jest zwiększenie liczby znaków hasła. Im większa minimalna liczba znaków, tym dłużej trwa złamanie hasła.
Oprócz korzyści płynących ze złożoności hasła, niesie to również pewne wyzwania. Jednym z głównych jest zapomnienie hasła. Trudno jest zapamiętać hasło, które jest dłuższe i zawiera znaki specjalne. Zwłaszcza, gdy wszystkie hasła są różne, trudno je zapamiętać i nie pomylić z innymi. Dlatego podczas tworzenia haseł należy przestrzegać pewnej logiki.

Na przykład;

- Jestem 2 dzieckiem w rodzinie z 3 dziećmi!

Możesz napisać takie zdanie w oparciu o własne prawdziwe życie. Kiedy weźmiesz pierwsze znaki i znaki specjalne zdania, otrzymasz hasło takie jak **Iat2ciafw3c!**

- Zostałem członkiem tej strony internetowej (o edukacji) 19 lipca.

Możesz dostosować zdanie takie jak "Zostałem członkiem tej strony (o edukacji) 20 grudnia" zgodnie z obszarem zainteresowań strony internetowej i datą członkostwa, abyś o tym nie

zapomniał. Kiedy dostaniesz ich pierwszą postać i znaki specjalne
Otrzymasz hasło takie jak **IBAMoTW(ae)oJ19.**

8. Zasady planu reagowania na zabezpieczenia

Plan reagowania na zabezpieczenia określa, co każdy zespół lub jednostka biznesowa musi zrobić w przypadku jakiegoś incydentu bezpieczeństwa, takiego jak naruszenie danych. Według SANS Institute powinien zdefiniować "opis produktu, informacje kontaktowe, ścieżki eskalacji, oczekiwane umowy dotyczące poziomu usług (SLA), klasyfikację ważności i wpływu oraz terminy łagodzenia / korygowania".

Kluczem do polityki planu reagowania na bezpieczeństwo jest to, że pomaga ona wszystkim różnym zespołom zintegrować ich wysiłki, tak aby każdy incydent bezpieczeństwa mógł zostać złagodzony tak szybko, jak to możliwe. Chociaż każdy dział może mieć własne plany reagowania, zasady planu reagowania na zabezpieczenia szczegółowo opisują, w jaki sposób będą koordynować się ze sobą, aby upewnić się, że reakcja na incydent bezpieczeństwa jest szybka i dokładna.

1.5. Przykłady polityki bezpieczeństwa informacji

Aby stworzyć udany plan bezpieczeństwa cybernetycznego, należy wziąć pod uwagę 5 głównych kwestii.

a. ***Identyfikacja:*** Organizacja powinna rozumieć zagrożenia cyberbezpieczeństwa, z którymi się boryka, aby mogła nadać priorytet swoim wysiłkom.

b. ***Ochrona***: Chodzi o wprowadzenie odpowiednich zabezpieczeń w celu ochrony zasobów danych i ograniczenia lub ograniczenia wpływu potencjalnego zdarzenia cybernetycznego. Obejmuje to edukację i wzmocnienie pozycji pracowników w organizacji, aby byli świadomi ryzyka, ustanowienie procedur, które koncentrują się na ochronie bezpieczeństwa sieci i aktywów oraz potencjalne wykorzystanie ubezpieczenia od odpowiedzialności cybernetycznej w celu ochrony finansowej firmy w przypadku, gdy cyberprzestępca jest w stanie ominąć istniejące zabezpieczenia.

c. ***Wykrywanie***: Nakreśl działania, które pomagają w wykryciu wystąpienia cyberataku i umożliwią szybką reakcję na zdarzenie. Aby szybko i skutecznie zdiagnozować cyberatak, firmy powinny wdrożyć klasyfikację danych, zarządzanie aktywami i protokoły zarządzania ryzykiem, które ostrzegają je, gdy dane wydają

się być zagrożone.

d. **Reagowanie**: Udokumentuj odpowiednie działania, które należy podjąć po wykryciu zagrożeń cyberbezpieczeństwa. Odpowiedź firmy powinna obejmować właściwą i dokładną komunikację z pracownikami, akcjonariuszami, partnerami i klientami, a także z organami ścigania i radcami prawnymi w razie potrzeby.

e. ***Odzyskiwanie***: Określ, w jaki sposób organizacja może odzyskać i przywrócić wszelkie możliwości lub usługi, które zostały uszkodzone w wyniku cyberataku.

Prawie każdy standard bezpieczeństwa musi zawierać wymóg dotyczący pewnego rodzaju planu reagowania na incydenty, ponieważ nawet najbardziej solidne plany bezpieczeństwa informacji i programy zgodności mogą nadal paść ofiarą naruszenia danych.

1.6. Ćwiczenia z Polityki Bezpieczeństwa Informacji

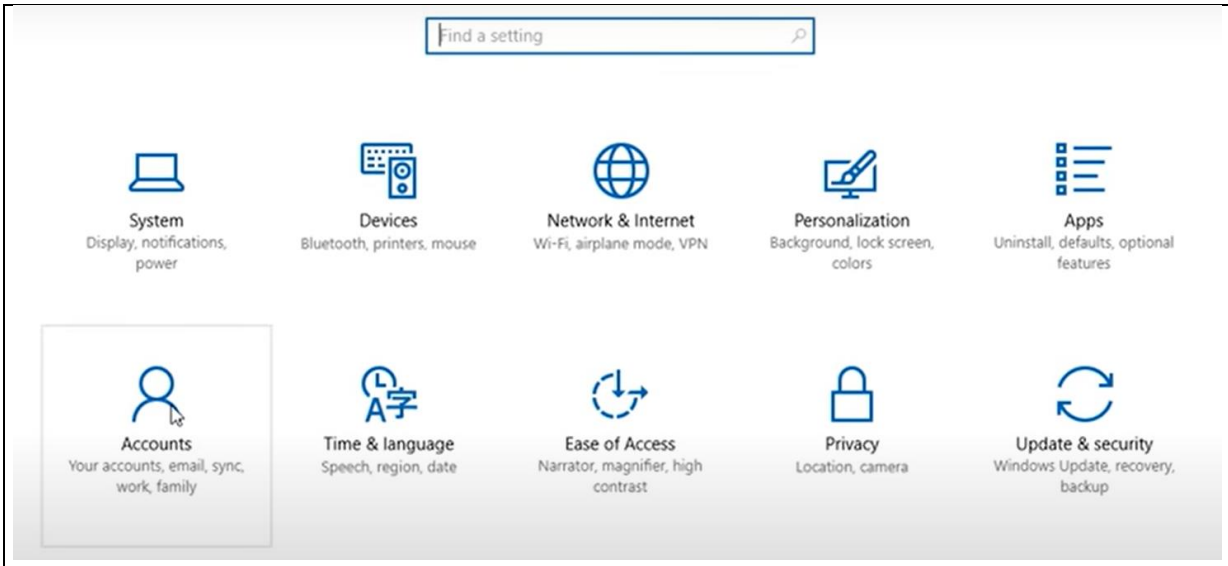
1. Zablokuj sesję: Wzmocnij swoje konta online, aktywując najsilniejsze dostępne narzędzia uwierzytelniające, takie jak biometria (mierzalne ślady biologiczne danej osoby), klucze bezpieczeństwa lub unikalny jednorazowy kod wygenerowany przez narzędzie aplikacyjne na urządzeniu mobilnym. Twoje nazwy użytkowników i hasła mogą nie być wystarczające do ochrony kont takich jak poczta e-mail, bankowość i media społecznościowe.

Ćwiczenie-1:

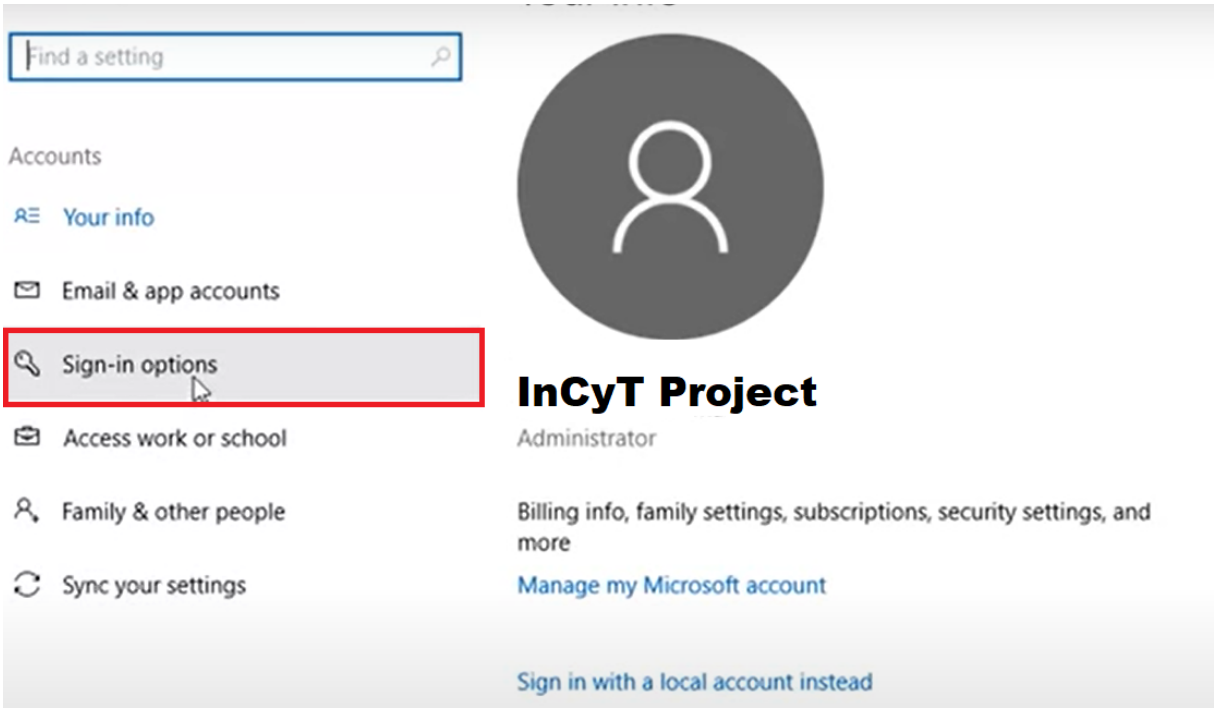
Aby komputer był automatycznie blokowany po odejściu od komputera.

Krok 1: Kliknij przycisk Ustawienia systemu.

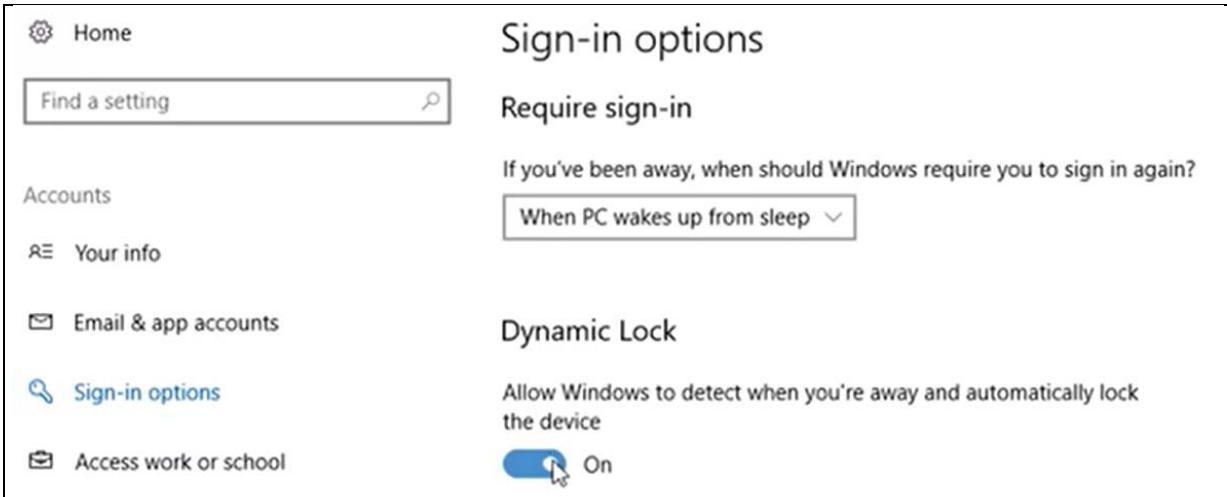
Krok 2: Kliknij kartę Konta.



Krok 3: Kliknij sekcję Zaloguj się.



Krok 4: Włącz Blokadę dynamiczną.



2- Utwórz silne hasło: Hasło ma ważne miejsce w bezpieczeństwie informacji. Słabe hasła można rozwiązać w krótkim czasie za pomocą programów do łamania haseł. Z tego powodu należy zachować najwyższą ostrożność, biorąc pod uwagę następujące zasady podczas tworzenia i używania haseł na wszystkich urządzeniach i kontach. Hasło jest powszechnie używane w wielu miejscach w systemach komputerowych. Używamy hasła podczas tworzenia konta e-mail, ustawiania hasła przy logowaniu komputera i zabraniania dostępu do plików. Jednak hasła nie powinny być słabe ani możliwe do odgadnięcia. Hasła powinny być tworzone według następujących kryteriów:

a. Hasła muszą mieć ***co najmniej 8 znaków*** i zawierać co najmniej jedną wielką literę, jedną małą literę, jedną cyfrę i jeden znak specjalny (.-+=_,!@$#*%<>[]{}).
b. Pole hasła ***nie powinno pozostawać*** puste ani domyślne; ***123456, 01062022, qwerty, password itp.*** nie należy go określać w taki sposób, aby był przewidywalny i łatwo łamliwy jak słowa, które można znaleźć w dowolnym słowniku.
c. Hasła nie powinny **zawierać danych osobowych** (imienia i nazwiska dziecka, daty urodzenia lub nazwy instytucji).
d. ***Należy*** utworzyć różne hasła dla różnych systemów i kont.
e. Hasła powinny być ***często zmieniane*** (co najmniej co 6 miesięcy).
f. Hasła nie powinny ***być zapisywane*** w miejscach, które mogą być zauważone przez inne osoby (np. pozostawiając je obok komputera, pisząc na papierze) i nie powinny być przechowywane w postaci zwykłego tekstu bez szyfrowania na komputerze lub na jakimkolwiek nośniku cyfrowym.
g. Żaden pracownik ani student nie powinien ***udostępniać*** swojego hasła (hasła e-mail, hasła do podpisu elektronicznego, hasła do komputera itp.) innej osobie. Użytkownicy powinni wiedzieć, że wszelka odpowiedzialność prawna, która może powstać w przypadku udostępniania, będzie należeć do niego.

h. Unikalne konto, unikalne hasło: Posiadanie osobnego hasła dla każdego konta pomaga udaremnić cyberprzestępców. Przynajmniej rozdziel swoje konta służbowe oraz osobiste i upewnij się, że Twoje krytyczne konta mają najsilniejsze hasła.
i. Pamiętaj i dbaj o bezpieczeństwo: Silne hasła są trudne do utworzenia i zapamiętania. Ustaw swoje hasła w sposób, który jest znaczący i niezapomniany tylko dla Ciebie, lub przechowuj je w bezpiecznym miejscu i formacie. Alternatywnie możesz użyć usługi, takiej jak menedżer haseł, aby śledzić swoje hasła.

Ćwiczenie-2:

Zabezpieczenie hasłem podczas tworzenia konta e-mail za pośrednictwem firmowego dostawcy usług poczty e-mail lub aplikacji lub witryny dostawcy publicznej poczty e-mail

Krok 1: Otwórz stronę internetową lub aplikację.
Krok 2: Wprowadź swoje dane osobowe, aby utworzyć konto.

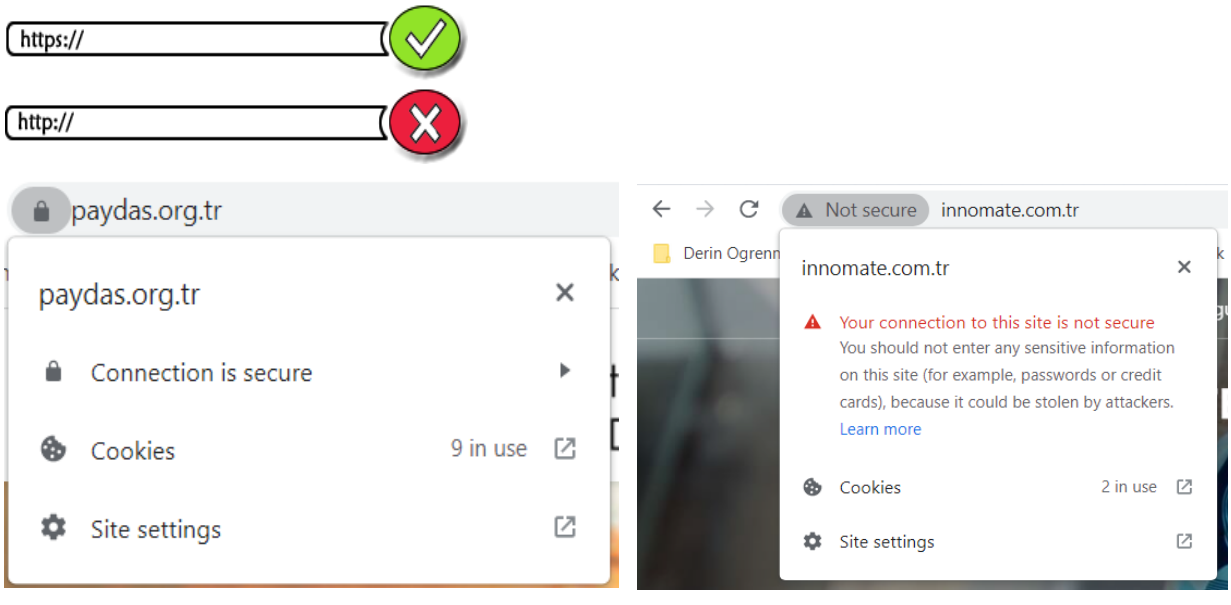
Krok 3: Podczas tworzenia hasła używaj kombinacji wielkich, małych liter, cyfr i symboli. Niektóre kodowanie można wykonać, aby hasło było łatwe do zapamiętania przez użytkownika. Na przykład możesz napisać zdanie odpowiednie dla tematu i użyć pierwszych znaków, liczb i

znaków specjalnych napisanego zdania.

This cybersecurity project is supported by Erasmus+ 2021

Krok 4: Ustawiamy nasze hasło; TcpisbE+2021
Krok 5: Upewnij się, że hasło składa się z co najmniej 8 znaków. Preferowane jest 12 znaków. Można powiedzieć, że hasło, którego używamy, jest odpowiednie, ponieważ ma 12 znaków.

3- Dostęp do bezpiecznych witryn (Bezpieczna przeglądarka): Kiedy idziesz na zakupy online lub czytasz wiadomości, używasz przeglądarki. Przeglądarki są jednym z podstawowych sposobów interakcji z Internetem. W rezultacie przeglądarki są głównym celem cyberprzestępców. Zawsze używaj najnowszej wersji przeglądarki i utrzymuj silną ochronę przed atakami przeglądarki. Zaktualizowane przeglądarki mają najnowsze poprawki bezpieczeństwa i są znacznie trudniejsze do wykorzystania przez cyberprzestępców. Nie masz pewności, czy masz najnowszą aktualizację przeglądarki? Skontaktuj się z zespołem pomocy technicznej lub zespołem ds. bezpieczeństwa informacji, aby dokonać weryfikacji. Zachowaj bezpieczeństwo w Internecie, nie łącząc się ze stronami internetowymi, gdy otrzymasz ostrzeżenie z przeglądarki. Nowoczesne przeglądarki mogą rozpoznawać niektóre złośliwe witryny internetowe, które mają na celu uszkodzenie/odczyt danych. Jeśli Twoja przeglądarka powiadomi Cię, że witryna, którą zamierzasz odwiedzić, jest niebezpieczna, zamknij tę stronę internetową i spróbuj znaleźć informacje, których szukasz, na bezpieczniejszej stronie internetowej. Przed wysłaniem poufnych informacji online, na przykład podczas wysyłania informacji o karcie kredytowej na zakupy online, upewnij się, że Twoja przeglądarka używa HTTPS, co jest oznaką szyfrowania. Szyfrowanie miesza informacje przesyłane między komputerem a miejscem docelowym, dzięki czemu tylko autoryzowana witryna może je odczytać. Aby uzyskać bezpieczne połączenie, poszukaj znaczników szyfrowania, takich jak adres witryny zaczynający się od HTTPS i ikona kłódki na pasku stanu.



Rys. 2. Bezpieczne i niezabezpieczone witryny sieci Web

Pytania:

1- Co nie jest jednym z elementów bezpieczeństwa informacji?

A) Poufność

B) Integralność

C) Luka w zabezpieczeniach

D) Dostępność

2- Która z poniższych instytucji nie jest jedną z instytucji określających politykę bezpieczeństwa informacji?

A) ENNISA

B) IPA

C) RODO

D) NIST

3- Które z poniższych nie ma bezpośrednio polityki bezpieczeństwa informacji dla organizacji?

A) Ochrona danych wrażliwych

B) Minimalizacja ryzyka incydentów związanych z bezpieczeństwem

C) Dostarczenie jasnego oświadczenia o bezpieczeństwie osobom trzecim

D) Obniżenie wymiaru czasu pracy pracowników

4- Które z poniższych nie są uwzględnione w bezpieczeństwie informacji?

A) Polityka sprzętowa

B) Polityka poczty elektronicznej

C) Polityka planu odzyskiwania po awarii

D) Polityka ochrony hasłem

5- Które z poniższych byłoby przykładem dobrze zdefiniowanego hasła?

A) 20220829

B) InCyT#2021!

C) Erasmus+

D) 123456!

6- Które z poniższych nie jest jednym ze środków, które należy podjąć w celu zapewnienia bezpieczeństwa informacji?

A) Preferuj strony internetowe https

B) Używanie silnego hasła

C) Odwiedzanie linków nieznanego pochodzenia

D) Oglądanie na ekranie komputera przez maksymalnie 8 godzin dziennie

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

- **Dlaczego polityka bezpieczeństwa informacji jest ważna?**
- ***Wyjaśnienie zasad ochrony hasłem***

Załączniki (prezentacja PowerPoint, materiały informacyjne, wydruki, linki, wideo...):

Zobacz załączniki

Odwołania:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/