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

Moduł treningowy InCyT

Bezpieczeństwo informacji dla menedżerów **Część 3, Tydzień 6** **Moduł: Bezpieczeństwo dostawców zewnętrznych**	
Zajęcia edukacyjne	❑ **Webinaria** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	• George Matache
Cele aktywności edukacyjnej	1. Zagrożenia w sieciach społecznych 2. Działania na rzecz bezpieczeństwa i prywatności w sieciach społecznościowych 3. Techniki bezpieczeństwa 4. Wymagania dotyczące zamówień
Umiejętności do zdobycia	• TS3 Bezpieczeństwo sieci • TS4 Testy penetracyjne (wykorzystujące podatności) • SS3 Analiza poznawcza i analiza zachowania
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest potrzebne?***
	• Podstawowe umiejętności w zakresie zarządzania • Podstawowe umiejętności informatyczne • Podstawowe umiejętności w zakresie bezpieczeństwa

Krótka informacja o module

Opis
Wymagania dotyczące zamówień publicznych odnoszą się do towarów i usług, które muszą być nabyte od organizacji spoza organizacji wykonującej. Z różnych powodów czasami organizacje wykonawcze polegają na sprzedawcach, którzy dostarczają to, co jest potrzebne do realizacji projektu. Na przykład rozważmy producenta widżetów, który podejmuje się realizacji projektu mającego na celu zautomatyzowanie systemu śledzenia zapasów. Niektóre z działań w ramach projektu obejmują przeniesienie pojemników w głównym magazynie. Niektóre z działań roboczych obejmują rozwój oprogramowania na zamówienie. Jeśli chodzi o działania związane z tworzeniem oprogramowania, producent widżetów nie dysponuje zasobami ludzkimi, które wiedziałyby, jak opracować aplikację. W odniesieniu do działań związanych z tworzeniem oprogramowania, producent widżetów musi zlecić te usługi. Sieci społecznościowe oparte na sieci Web (WBSN) to społeczności internetowe, które umożliwiają użytkownikom publikowanie zasobów (np. danych osobowych, adnotacji, blogów) oraz nawiązywanie relacji, możliwie różnego typu, w celach, które mogą dotyczyć biznesu, rozrywki, religii, randek itp. W ciągu ostatnich kilku lat wzrasta wykorzystanie i rozpowszechnienie WBSN, a około 300 serwisów internetowych gromadzi informacje ponad 400 milionów zarejestrowanych użytkowników. W rezultacie, "model sieciowy" jest dziś coraz częściej wykorzystywany do komunikacji, wymiany informacji, podejmowania decyzji i "robienia interesów" przez firmy i organizacje. Wyzwaniem staje się więc opracowanie mechanizmów bezpieczeństwa dla sieci społecznościowych, zdolnych do ochrony prywatnych informacji i regulowania dostępu do współdzielonych zasobów. W niniejszym artykule, oprócz przedstawienia charakterystyki środowiska WBSN i jego wymagań w zakresie ochrony, ilustrujemy obecne podejścia i przyszłe trendy w zakresie bezpieczeństwa sieci społecznych, ze szczególnym uwzględnieniem pojawiających się technologii związanych z tzw. Web 2.0. Słuchacze mogli uzyskać informacje na temat tych aspektów czytając odpowiedni tekst, oglądając streamingowe webinaria i rozwiązując ćwiczenia we własnym tempie. Wszystkie te dokumenty znajdują się na cyfrowej interaktywnej platformie projektu. Słuchacze mogą sprawdzić swoje odpowiedzi na ćwiczeniach Samooceny. Odpowiedzi na inne ćwiczenia powinny być zapisywane na odpowiednim forum dyskusyjnym i omawiane z mentorem

podczas wspólnych spotkań organizowanych raz w tygodniu. Słuchacze mogą współpracować z innymi słuchaczami i mentorem, szczególnie podczas spotkań. Będą wspierani w tworzeniu e-portfolio ważnego dla refleksji i oceny szkolenia.

Treść materiału edukacyjnego

Dostawca zewnętrzny to osoba lub firma, która świadczy usługi dla innej firmy (lub klientów tej firmy). Podczas gdy dostawcy są uważani za "strony trzecie", niektóre branże odróżnić "dostawca strony trzeciej" szczególnie jako dostawca na podstawie pisemnej umowy, ale nie wszyscy dostawcy pracują na podstawie umowy. Dla jasności, termin " dostawca strony trzeciej " w tym artykule odnosi się do każdej osoby lub firmy, która świadczy usługi dla innej firmy z lub bez umowy.

Współpraca jest kluczem do sukcesu. Współpraca ze stronami trzecimi pomaga firmom zwiększyć produktywność i wydajność, wytwarzać lepsze produkty i usługi, zatrudniać wysoko wykwalifikowanych ekspertów i obniżać koszty. Jednak wszystkie te korzyści mają swoją cenę w postaci zwiększonego ryzyka związanego z bezpieczeństwem cybernetycznym. Drobne błędy w procedurach bezpieczeństwa i prywatności dostawcy zewnętrznego mogą przekształcić się w słabości cyberbezpieczeństwa dla Twojej firmy. W tym artykule analizujemy poszczególne zagrożenia cyberbezpieczeństwa związane z podmiotami zewnętrznymi oraz sposoby ich ograniczania.

Towary i usługi uzyskane od sprzedawców zewnętrznych mogą obejmować, ale nie ograniczają się do:

- Usług hostingowych w chmurze. Sprzedawca usług hostingowych w chmurze może zapewnić wszystko, od przestrzeni dyskowej i przepustowości do szyfrowania i zaawansowanych technologicznie rozwiązań bezpieczeństwa.
- Rozwiązania programowego w chmurze. Sprzedawcy oprogramowania SaaS zapewniają dostęp do programów dla Twojej firmy lub Twoich klientów. Na przykład, platformy automatyzacji marketingu, CRM, pakiety księgowe itp.
- Konserwacji sprzętu. Firma, która naprawia Twoją kserokopiarkę i zespół, który zarządza bezpieczeństwem Twojej sieci to dostawcy zewnętrzni.
- Serwisowania HVAC (ogrzewanie, wentylacja itp.). Lokalna firma HVAC, która serwisuje Twoje urządzenie, świadczy usługi sprzedawców zewnętrznych.
- Podwykonawców każdego rodzaju. Każdy wykonawca, krótko- lub długoterminowy, jest sprzedawcą strony trzeciej.
- Dostawców call center. Jeśli hostujesz swoje call center z inną firmą, jest ona uważana za sprzedawcę zewnętrznego.
- Księgowych/ audytorów finansowych. Każda osoba lub firma zatrudniona do zarządzania

Twoimi finansami, budżetem lub audytem finansowym jest sprzedawcą zewnętrznym.

- Prawnicków. Czasami konieczne jest skonsultowanie się z prawnikiem przed podpisaniem umów lub dokonaniem dużych zakupów. Wszystkie usługi prawne są uważane za sprzedawców zewnętrznych.

Ponieważ organizacje w coraz większym stopniu polegają na zewnętrznych dostawcach w celu zapewnienia podstawowych usług, stają się również bardziej podatne na zagrożenia cybernetyczne związane z dostawcami. Ostatnie badanie wykazało, że prawie 60% firm doświadczyło naruszenia danych z powodu dostawcy zewnętrznego w ciągu ostatniego roku. Ale jakie są najczęstsze cyber luki związane z dostawcami, o których organizacje powinny wiedzieć?

Jakie są korzyści z korzystania z usług zewnętrznych dostawców dla usługodawców?

W dzisiejszym świecie nie sposób uniknąć korzystania z usług zewnętrznych dostawców. Bez względu na to, ile działów stworzy Twoja firma, nigdy nie pokryjesz wszystkich usług, których kiedykolwiek będziesz potrzebować. Nie powinno to mieć miejsca, ponieważ firmy muszą określić właściwą równowagę pomiędzy umiejętnościami, które są niezbędne dla biznesu, a tymi, które można zlecić na zewnątrz. Oto, co się dzieje, gdy uda się zachować właściwą równowagę:

Zaoszczędzisz czas. Nikt nie ma czasu, aby nauczyć się każdej umiejętności lub zatrudnić każdą osobę niezbędną do prowadzenia firmy. Sprzedawcy zewnętrzni sprawiają, że procesy biznesowe przebiegają sprawnie, pozyskując wszystkie profesjonalne usługi wymagane do obsługi i realizacji zamówień dla Twoich klientów.

Zaoszczędzisz pieniądze. Być może największą korzyścią jest oszczędność kosztów. Kontraktowanie dostawcy zewnętrznego do pracy w miarę potrzeb może być znacznie mniej kosztowne niż posiadanie zawsze specjalistów na liście płac firmy. Na przykład, znacznie mniej kosztowne jest wynajęcie prawnika, gdy jest on potrzebny, niż utrzymywanie go na etacie.

Zyskasz cenne doświadczenie. Twoja firma nie ma czasu na tworzenie nowego zespołu ekspertów. Czas i koszty takiego działania byłyby ogromne. Wynajęcie dostawcy zewnętrznego w celu uzyskania wiedzy specjalistycznej, której nie masz we własnym zakresie, prawdopodobnie przyniesie lepsze rezultaty.

Jakie są zagrożenia związane z korzystaniem z usług dostawców zewnętrznych?

Osoby trzecie mogą nie traktować bezpieczeństwa swojej sieci tak poważnie, jak byśmy tego chcieli. Wiedząc o tym, hakerzy mogą zdecydować się nie atakować bezpośrednio Twojej firmy. Zamiast tego mogą szukać łatwiejszego celu wśród dostawców zewnętrznych. Skompromitowany podwykonawca może łatwo stać się punktem wejścia dla cyberprzestępców.

Jeśli Twoi dostawcy nie wywiążą się z umowy, Ty również nie wywiążesz się z umowy. Jednak ryzyko

jest nieodłącznym elementem każdej relacji biznesowej. Korzystanie z usług zewnętrznych dostawców wiąże się z wieloma zagrożeniami, z których większość można ograniczyć.

Największym ryzykiem jest wybór relacji ze stroną trzecią, która nie jest zgodna z Twoimi standardami bezpieczeństwa. Na przykład, zespół ds. bezpieczeństwa sieci musi przestrzegać protokołów bezpieczeństwa, które spełniają określone standardy. Jeśli Twoja firma jest związana przepisami, takimi jak ubezpieczenie zdrowotne, nie możesz sobie pozwolić na zatrudnienie firmy zajmującej się bezpieczeństwem sieci, która nie spełnia przepisów dotyczących bezpieczeństwa danych medycznych. Potrzebujesz dostawcy, który rozumie przepisy i jest gotów dostosować się do nich.

Kiedy jesteś związany przepisami dotyczącymi prywatności danych, musisz wiedzieć dokładnie, jakie standardy bezpieczeństwa są wdrażane i jeśli twoi dostawcy nie są na równi z nimi, musisz spróbować to naprawić. W przeciwnym razie, narażasz swoją firmę na ryzyko związane z bezpieczeństwem cybernetycznym, takie jak naruszenie danych.

Naruszenia danych są niezwykle destrukcyjne, zwłaszcza gdy chronisz dane osobowe. Niestety, liczba naruszeń danych wzrasta i są one bardziej powszechne niż kiedykolwiek wcześniej. Naruszenia danych mogą powodować zakłócenia w działalności, niszczące konsekwencje finansowe, działania prawne i utratę reputacji. Aby tego uniknąć, nie można opuszczać gardy, jeśli chodzi o bezpieczeństwo własne lub swoich dostawców.

W zależności od charakteru kompromisu z dostawcą zewnętrznym, organizacja może być narażona na różne ryzyka. Przyjrzyjmy się najczęstszym kategoriom ryzyka i zagrożeniom, na które należy być przygotowanym, aby je ograniczyć. Skompromitowany dostawca zewnętrzny może prowadzić do wielu zagrożeń, które można podzielić na cztery główne kategorie: Rys. 1

Ryzyko związane z cyberbezpieczeństwem - podwykonawcy zazwyczaj mają legalny dostęp do różnych środowisk, systemów i danych swoich klientów. Atakujący mogą wykorzystać dostawcę zewnętrznego jako punkt wejścia do próby zdobycia Twoich cennych zasobów.

Ryzyko operacyjne - Cyberprzestępcy mogą obrać za cel nie tylko dane, ale także wewnętrzne systemy i usługi, z których korzystasz. Może to prowadzić do częściowego przerwania działalności lub nawet całkowitego jej wstrzymania.

Ryzyko zgodności - Międzynarodowe, lokalne i branżowe normy oraz przepisy określają surowe kryteria bezpieczeństwa cybernetycznego, które organizacje powinny spełniać. Co więcej, strony trzecie współpracujące z tymi organizacjami również muszą przestrzegać tych wymogów. Niezgodność z przepisami zwykle prowadzi do znacznych kar pieniężnych i utraty reputacji.

Ryzyko utraty reputacji - Narażenie cennych danych i systemów stanowi czerwoną flagę dla partnerów i klientów, zarówno obecnych, jak i przyszłych. Odzyskanie ich zaufania wymaga wiele czasu i wysiłku. Niestety, nie ma gwarancji, że uda się odzyskać reputację po poważnym incydencie związanym z bezpieczeństwem cybernetycznym.

Wymagania dotyczące zamówień

Z różnych powodów, czasami organizacje wykonawcze polegają na dostawcach, aby zapewnić to, co jest potrzebne do ukończenia projektu. Szczególnie dotyczy to małych i średnich przedsiębiorstw. Wymagania dotyczące zamówień są zatem niezwykle ważne w pracy z bezpieczeństwem dostawców zewnętrznych.

Chociaż prawdą jest, że zamówienia są procesem wysoce zindywidualizowanym, istnieje również kilka podstawowych etapów, które będą generalnie wykorzystywane w całej sprawie.

Wymagania dotyczące zamówień odnoszą się do towarów i usług, które muszą być nabyte od organizacji spoza organizacji wykonującej. Z różnych powodów, czasami organizacje wykonawcze polegają na dostawcach w celu zapewnienia tego, co jest potrzebne do realizacji projektu.

Etapy procesu zamówień publicznych
Etap 1: Zidentyfikowanie zapotrzebowania na produkty i/lub usługi.
Etap 2: Stworzenie i złożenie wniosku o zakup.
Etap 3: Ocena i wybór dostawców/dostawców.
Etap 4: Negocjowanie warunków umowy z wybranym dostawcą.
Etap 5: Sfinalizowanie zamówienia zakupu.

Pierwszym krokiem w procesie zamówień jest identyfikacja wymagań. Wszystkie wymagania dotyczące zamówień publicznych zaczynają się od dostrzeżenia potrzeby. Potrzeba przekroczenia zbiornika wodnego może stworzyć wymóg budowy mostu, promu lub innych systemów transportowych.

Etap 1: Określenie zapotrzebowania na produkty i/lub usługi
Zanim rozpocznie się proces zaopatrzenia, należy rozpoznać konkretną potrzebę. Na przykład, organizacja może być zainteresowana zakupem nowych monitorów komputerowych, ponownym zamówieniem miesięcznych dostaw produktów papierniczych lub nabyciem zaktualizowanego oprogramowania. W zależności od struktury firmy, ten etap może być zarządzany przez właścicieli firmy, szefów działów, zespół wykonawczy, personel i / lub menedżerów zamówień. Na tym etapie ustalany jest budżet i często dokonywana jest ocena kompleksowego spojrzenia na wydatki.

Na tym etapie konieczne jest jasne zdefiniowanie potrzeby, co może być dokonane za pomocą badania w celu określenia najlepszego sposobu przekroczenia zbiornika wodnego (biorąc pod uwagę obecną sytuację i przewidywane przyszłe potrzeby), następnie rodzaju mostu, który ma być zbudowany lub analizy porównawczej kosztów i korzyści w celu określenia najlepszego rozwiązania pomiędzy mostem a innymi alternatywami. Studium powinno zawierać informację, czy potrzeby mogą być zaspokojone we własnym zakresie, czy też na zlecenie, kwantyfikację wstępnych szacunków budżetowych oraz pomysł na czas realizacji zamówienia.

Etap 2: Utworzenie i złożenie wniosku o zakup
Wniosek o zakup (lub zapotrzebowanie na zakup) jest formalnym wnioskiem o towary lub usługi i jest zazwyczaj składany przy użyciu specjalistycznego oprogramowania do zamówień publicznych. Często wniosek o zakup pochodzi od pracownika lub menedżera, a następnie jest przeglądany przez

zespół zamówień publicznych organizacji.

Kiedy wniosek o zakup jest zatwierdzony, staje się zamówieniem usługi/towaru. Jednakże, jeśli wniosek zostanie odrzucony, to zazwyczaj zostanie zwrócony do wnioskodawcy z krótkim wyjaśnieniem. Odrzucone zamówienie zakupu, choć nie jest idealne, może być dobrą okazją do nauki.

Etap 3: Ocena i wybór dostawców/wykonawców
Kolejnym krokiem jest ocena różnych dostawców, a następnie wybranie takiego, który spełnia kluczowe wymagania. Niektóre organizacje utrzymują katalog zatwierdzonych dostawców, w którym znajdują się różni dostawcy, którzy już się sprawdzili.

Pozyskiwanie dostawców to proces, który może być od prostego do złożonego, z jego zakresem określonym przez wymagania. Zazwyczaj kilka zapytań ofertowych (RFQ) zostanie wysłanych do różnych dostawców, aby organizacja/zespół ds. zamówień publicznych mógł porównać ceny i opcje.

Pamiętaj, że cena nie powinna być jedynym wyznacznikiem przy wyborze dostawcy. Aby uzyskać najlepsze wyniki, należy rozważyć "szerszą perspektywę" tego, co sprzedawca może zaoferować, w tym:

- Łatwość komunikacji
- Etyka przedsiębiorstwa
- Odpowiedzialność
- Zdolności produkcyjne

Po wybraniu dostawcy ważne jest zainwestowanie czasu i energii w relację. Dobre relacje z dostawcą mogą odblokować lepsze oszczędności i usługi, zapewniając maksymalną wartość w dłuższej perspektywie.

Etap 4: Negocjowanie warunków umowy z wybranym dostawcą
Gdy już wybrałeś najlepiej dopasowanego dostawcę, czas przejść do negocjacji kontraktu. W kontekście udanego zakupu jest to jeden z najbardziej krytycznych etapów. To w tym etapie, że będzie zarys ceny, jak również szczegóły, takie jak harmonogramy dostaw, szczególne warunki i więcej szczegółów. Często przydatna jest ocena poprzednich umów, aby wskazać możliwości poprawy, co pozwoli Ci na bardziej świadome podejście w przyszłości.

Etap 5: Finalizacja zamówienia zakupu

Po zatwierdzeniu ostatecznej umowy, kolejnym etapem jest zamówienie zakupu (PO, ang. *Purchase order*). Umowa zazwyczaj reguluje pełną relację kupujący/dostawca, natomiast zamówienie zakupu przybliża się do konkretnego zakupu.
Pomyśl o tym dokumencie jako o kolejnym formalnym kontrakcie, który w pełni precyzuje następujące kwestie:

- Całkowite koszty/cenę
- Szczegółowy opis towarów i/lub usług
- Ilość
- Wszelkie inne specyficzne warunki i zasady

Etap 6: Zarządzanie zamówieniami
W miarę dostarczania towarów/usług powinna zostać wybrana osoba odpowiedzialna, najlepiej użytkownik końcowy produktu lub usługi, za sprawdzenie, czy wszystkie standardy zostały spełnione terminy dostaw, ilość produktów, jakość itp. Jeśli wystąpią problemy z przedmiotami (np. uszkodzone produkty), użytkownik ma możliwość odrzucenia dostawy. Jasna komunikacja z dostawcą jest kluczowa w przypadku jakichkolwiek problemów z dostawą.

Ponieważ technologia i komunikacja pozwalają firmom na rozszerzenie ich łańcuchów dostaw, złożoność zarządzania ryzykiem związanym z dostawcami wzrasta. Twoja firma prawdopodobnie współpracuje z większą liczbą dostawców niż kiedykolwiek wcześniej, a każdy z tych dostawców będzie stanowił pewien poziom ryzyka dla Twojej organizacji.

Zarządzanie ryzykiem bezpieczeństwa dostawców to strategia mająca na celu ograniczenie liczby zagrożeń, podatności i słabości, z jakimi boryka się organizacja z powodu dostawców w łańcuchu dostaw. Sprzedawca to zazwyczaj organizacja będąca stroną trzecią, która sprzedaje produkt, usługę lub element wyposażenia, którego firma potrzebuje do działania.

Każdy dostawca, po podłączeniu do Twojej organizacji, będzie ponosił pewien poziom ryzyka związanego z bezpieczeństwem cybernetycznym. Jeżeli nie dotrzyma on warunków umowy lub padnie ofiarą cyberataku, może to mieć bezpośredni wpływ na Twoją organizację. Skuteczna ocena ryzyka, jako część większego planu zarządzania ryzykiem dostawcy, stara się zidentyfikować te potencjalne punkty awarii na długo zanim staną się problemem i naprawić je.

Cykl zarządzania ryzykiem dostawcy
Zarządzanie ryzykiem związanym z bezpieczeństwem dostawców jest procesem ciągłym, który należy przeprowadzać z każdym dostawcą wprowadzanym do łańcucha dostaw. Zazwyczaj proces ten wygląda następująco:

Krok 1: Analiza - Firma identyfikuje nieodłączne ryzyko związane z relacją oraz poziom należytej

staranności, który należy przeprowadzić. W związku z tym firma ocenia postawę bezpieczeństwa strony trzeciej i przeprowadza analizę luk.
Krok 2: Zaangażowanie - firma i strona trzecia współpracują nad sposobem usunięcia luk.
Krok 3: Naprawa - strona trzecia usuwa luki cybernetyczne.
Krok 4: Zatwierdzenie - firma zatwierdza stronę trzecią lub odrzuca ją w oparciu o tolerancję ryzyka.
Krok 5: Monitorowanie - firma kontynuuje monitorowanie strony trzeciej w celu wykrycia wszelkich luk cybernetycznych.

Sieci społecznościowe i zagrożenia bezpieczeństwa sprzedawców

Sieci społecznościowe są bardzo popularne w dzisiejszym świecie. Zazwyczaj sieć społecznościowa jest definiowana jako sieć małego świata, składająca się ze zbioru jednostek (osób, grup, organizacji) połączonych relacjami osobistymi, zawodowymi lub relacjami zaufania. Sieć społecznościowa jest więc pojęciem dość szerokim i ogólnym, które w kontekście sieci może być stosowane do każdego rodzaju społeczności wirtualnej. Na przykład, użytkownicy zarejestrowani w serwisie internetowym, takim jak poczta internetowa, czasopisma online lub gazety wymagające prenumeraty, mogą być uważani za sieć społecznościową. W dalszej części przyjmujemy definicję, zgodnie z którą serwis internetowy społeczności internetowej może być uznany za sieciową sieć społecznościową tylko wtedy, gdy spełnia następujące warunki:

- Relacje są wyraźnie określone przez członków, a nie wywnioskowane z istniejących interakcji (np. lista mailingowa może być użyta do wywnioskowania ukrytych relacji).
- Relacje są przechowywane i zarządzane przy użyciu technologii, takich jak systemy zarządzania bazami danych, pozwalających na analizę relacji oraz regulujących dostęp i pobieranie danych o relacjach.
- Członkowie są w stanie uzyskać dostęp do informacji o relacjach, przynajmniej częściowo.

Kluczowe pojęcia

Relationship-Based Access Control: Paradygmat kontroli dostępu specjalnie dostosowany do sieci społecznych, zgodnie z którym członkowie sieci społecznej upoważnieni do dostępu do danego zasobu są oznaczani pod względem relacji, w których muszą uczestniczyć, aby uzyskać dostęp.

Sieć społeczna: Sieć małego świata składająca się ze zbioru jednostek (osób, grup, organizacji) połączonych relacjami osobistymi, zawodowymi lub zaufaniem. Zazwyczaj modelowana jako graf, gdzie węzły odpowiadają członkom sieci społecznej, natomiast krawędzie oznaczają istniejące między nimi relacje.

Sieci społeczne. Komunikacja i dzielenie się informacjami z osobami wokół nas jest częścią życia każdego z nas i ewoluowała od prostych wiadomości tekstowych, poprzez e-maile, aż do tego, co obecnie nazywamy platformami mediów społecznościowych. To, co nie jest zbyt dobrze znane lub uświadomione, to fakt, że nasza ekspozycja w środowisku online wiąże się z wieloma zagrożeniami.

Media społecznościowe i aplikacje do obsługi sieci społecznościowych lub komunikatorów mogą stanowić szereg zagrożeń dla bezpieczeństwa i prywatności zarówno dla organizacji, jak i osób fizycznych, jeśli są wykorzystywane w niewłaściwy lub niebezpieczny sposób. Najbardziej popularne i rozpowszechnione platformy w sieciach społecznościowych:

- Facebook posiadający ponad 1 300 000 000 użytkowników;
- Flickr używany do przechowywania, organizowania i udostępniania plików multimedialnych;
- LinkedIn z ponad 300 milionami użytkowników;
- Instagram z ponad 30 milionami użytkowników;
- Twitter z ponad miliardem użytkowników;
- YouTube z ponad miliardem użytkowników;
- Tinder z około 12 milionami użytkowników;
- TikTok z ponad 800 milionami użytkowników.

Kontrola dostępu z uwzględnieniem prywatności: W kontekście sieci społecznościowych oznacza paradygmat kontroli dostępu, w którym wymogi kontroli dostępu członków sieci społecznościowych są egzekwowane bez ujawniania prywatnych informacji o relacjach, w których uczestniczą.

Sieć społeczna oparta na sieci Web: System oparty na sieci Web, który umożliwia swoim zarejestrowanym członkom nawiązywanie relacji z innymi członkami oraz dzielenie się różnymi rodzajami informacji (np. danymi osobowymi, kontaktami, zasobami multimedialnymi).

Analiza sieci społecznych: Dyscyplina mająca na celu zbieranie danych statystycznych z analizy topologii sieci społecznych.

Poziom zaufania do relacji: W sieci społecznej oznacza wartość związaną z relacją zaufania, stanowiącą miarę tego, jak bardzo dany członek uważa innego członka za godnego zaufania. W zależności od celu, w jakim jest używane, pojęcie to może mieć różne znaczenia. Na przykład w środowisku oceny współpracy oznacza ono, jak bardzo dany członek ufa opiniom innego członka w odniesieniu do konkretnego tematu (zaufanie tematyczne) lub ogólnie (zaufanie absolutne). Natomiast w kontekście kontroli dostępu ma pewne podobieństwa do pojęcia poziomu bezpieczeństwa stosowanego w modelach kontroli dostępu obowiązkowego.

Perturbacja krawędziowa: Technika anonimizacji grafu mająca na celu ukrycie rzeczywistych relacji w sieci społecznej poprzez wykonanie zestawu losowych usunięć/wstawień krawędzi w grafie sieci.
Relacja w sieci społecznej: Relacja dotycząca dwóch członków sieci społecznej. W WBSNs, poza relacjami osobistymi/pracownika (np. przyjaciel/kolega), mogą występować również relacje zaufania, które określają jak bardzo jeden członek ufa drugiemu. W graficznej reprezentacji sieci społecznej, relacje są zwykle oznaczane przez krawędzie, opatrzone etykietą typu relacji i/lub

poziomu zaufania.

Anonimizacja grafu: Technika mająca na celu ukrycie prywatnych informacji o członkach sieci społecznej podczas przeprowadzania analizy sieci społecznej. Anonimizacja węzłów i perturbacja krawędzi to dwie główne techniki anonimizacji grafu stosowane obecnie.

Anonimizacja węzła: Technika anonimizacji grafu mająca na celu ukrycie tożsamości członków sieci społecznej poprzez oznaczenie odpowiadających im węzłów losowymi identyfikatorami (anonimizacja naiwna) lub, w przypadku gdy węzły są powiązane z atrybutami, które mogą być wykorzystane do identyfikacji odpowiadającego im użytkownika, poprzez zastosowanie technik opartych na k-anonimowości (Sweeney, 2002).

Ryzyko

Geotagowanie

- Oznacza dodawanie danych geoidentyfikacyjnych do zdjęć, filmów, stron internetowych i wiadomości tekstowych przez aplikacje, które mogą odczytać lokalizację użytkownika lub które mają taką możliwość w ustawieniach użytkownika;
- Pamiętaj o wyłączeniu funkcji geotagowania w newralgicznych miejscach, aby uniknąć ujawnienia dokładnej lokalizacji, miejsca pracy lub zamieszkania.

"Publika"

- Jest to ogólny termin, który odnosi się do tego, kto jest w stanie zobaczyć i/lub skomentować Twoje posty;
- Twoja grupa znajomych może w każdej chwili zmienić się i być w stanie zobaczyć post zawierający informacje o Tobie. Możesz celowo podzielić się czymś ze swoimi "przyjaciółmi", ale to, co oni zrobią z tym postem, jest poza Twoją osobistą kontrolą.

Tożsamość

- Opisuje zakres informacji, które konkretnie odnoszą się do danej osoby;
- Należy pamiętać, że są osoby, które wykorzystują media społecznościowe jako metodę badawczą do poszukiwania informacji o tożsamości, z możliwym złym zamiarem, takim jak kradzież tożsamości, oszustwo, defraudacja lub zastraszanie.

Środki zaradcze

Hasło

- Zaleca się stosowanie innego hasła do każdego konta internetowego;
- Powinno mieć długość co najmniej 10 znaków i zawierać duże litery, małe litery, cyfry i znaki specjalne;

- Nie wolno go nikomu ujawniać, niezależnie od tego, jak bliska lub zaufana jest osoba, której chcemy je przekazać
- Zaleca się, aby przy tworzeniu hasła nie używać informacji osobistych (np.: imiona rodziców, data urodzenia, imię zwierzęcia domowego itp;)
- Okresowo zmieniać swoje hasło;
- Wyloguj się ze swojego konta, gdy korzystasz z urządzenia, które nie należy do Ciebie lub jest używane przez kogoś innego.

Wykonuj aktualizacje zabezpieczeń na czas!

- Platformy mediów społecznościowych regularnie wprowadzają nowe ustawienia prywatności i bezpieczeństwa. Można je znaleźć w ustawieniach konta i zaleca się ich regularne sprawdzanie;
- Korzystaj z opcji uwierzytelniania dwuskładnikowego (2FA), aby mieć pewność, że ktoś nie próbuje zhakować Twojego konta.

Nie akceptuj próśb o przyjaźń od każdego!

- Akceptuj lub wysyłaj prośby o przyjaźń tylko od/do osób, które spotykasz w prawdziwym życiu lub do osób publicznych, którymi jesteś zainteresowany, dbając o śledzenie ich oficjalnych profili;
- NIE ZAPOMINAJ! Jeśli czujesz się przywiązany do pewnych kont, możesz ograniczyć ich dostęp do swoich postów lub możesz zablokować konto. Masz również możliwość zgłaszania kont lub postów z powodów takich jak: fałszywe konto, fałszywa nazwa, posty o nieodpowiedniej treści, nawoływanie do przemocy, fałszywe informacje itp.
- NIE klikaj!
- Wielu napastników wykorzystuje inżynierię społeczną do zdobycia zaufania danej osoby, aby później uzyskać dostęp do informacji;
- Nie otwieraj linków i załączników z mediów społecznościowych, jeśli nie jesteś w 100% pewien źródła (np. strony oferujące nagrody często mają na celu kradzież informacji);
- Jeśli z czatów znajomy wydaje się zachowywać inaczej (zadaje dużo pytań, staje się bardzo ciekawy życia osobistego, prosi o pieniądze) istnieje możliwość, że jego konto zostało zhakowane i napastnik wykorzystuje je do złych celów.

Zastanów się dwa razy zanim napiszesz post!

- Media społecznościowe dają tyle samo możliwości tworzenia pozytywnej reputacji w sieci, co negatywnej, dodatkowo nawet jeśli "usuniemy" jakiś post, to po pojawieniu się w sieci nie można go trwale usunąć;
- Nie ujawniaj zbyt wielu danych osobowych w mediach społecznościowych! Pola "O mnie" są nieobowiązkowe.
- Ustal granicę między życiem zawodowym a osobistym w środowisku online
- Nie ujawniaj online informacji o swoim pracodawcy
- Nie zamieszczaj zdjęć z pracy ani negatywnych wiadomości, które stawiają pracodawcę w złym świetle.

- Pomyśl, zanim zamieścisz post i nie ryzykuj swojej pracy.

Zamknij stare konta!

- Jeśli masz stare konta na platformach społecznościowych, których już nie używasz, a nawet stare konta na tej samej platformie, spróbuj je zamknąć. W ten sposób tworzysz jak najmniej powiązań, przy czym obecne konta są bardziej chronione przed ewentualnymi napastnikami;
- Starsze konta lub platformy mogą nie być tak bezpieczne jak dzisiejsze.

Media społecznościowe stwarzają duże zagrożenia

- Sieci społecznościowe stanowią duże zagrożenie dla bezpieczeństwa i prywatności ze względu na ich scentralizowaną architekturę, ogromny magazyn informacji umożliwiających identyfikację osób, które każdy haker chciałby mieć, oraz ogólną niewiedzę ludności na temat właściwego korzystania z mediów społecznościowych. ustawienia prywatności w celu poprawy ich bezpieczeństwa online.
- Innym bardzo wysokim ryzykiem, szczególnie wśród nastolatków, jest zaufanie do innych ludzi i rodzaju informacji osobistych ujawnianych online.
- Można z tym walczyć poprzez środki technologiczne i egzekwowanie polityki bezpieczeństwa.
- Powinniśmy uznać, że informacje przekazywane za pośrednictwem mediów społecznościowych nie są bezpieczne i dlatego nie przekazujemy wrażliwych informacji za pośrednictwem mediów społecznościowych, dlatego główna odpowiedzialność za zachowanie bezpieczeństwa spoczywa na UŻYTKOWNIKU

Złe nawyki w mediach społecznościowych

- Portale społecznościowe to dziś powszechnie wykorzystywane przez użytkowników platformy. Mamy do dyspozycji szeroki wachlarz możliwości.
- Niektóre są bardziej nastawione na pubikowanie zdjęć lub filmów, inne na nasze opinie, a w jeszcze innych przypadkach po prostu na utrzymywanie kontaktu z przyjaciółmi i rodziną. W każdym przypadku mamy do czynienia z platformami, które mają wielu użytkowników na całym świecie.
- To również sprawia, że hakerzy ustawiają tutaj swoje celowniki. Porozmawiamy o tych nawykach, które należy zmienić w sieciach społecznościowych, jeśli chcemy zachować naszą prywatność i bezpieczeństwo.
- Istnieje wiele rodzajów platform, które możemy znaleźć w sieci, które dają nam możliwość wysyłania wiadomości do przyjaciół lub rodziny, komentowania zdjęć, filmów ...
- To sprawia, że są one bardzo popularnym środowiskiem zarówno dla użytkowników prywatnych, jak i firm.
- Powoduje to jednak również pewne ryzyko dla naszego bezpieczeństwa i prywatności. Hakerzy mogą obserwować tutaj, jak przeprowadzają swoje ataki. Szczególnie mogą wykorzystać złe nawyki użytkowników podczas korzystania z tych platform.

Nawyki, które należy zmienić

- Prywatność i bezpieczeństwo to bardzo ważne czynniki dla użytkowników.
- Jednak nie zawsze są one obecne.
- Możemy stać się ofiarami wielu rodzajów ataków, które narażają te dwa czynniki.
- Możemy również popełniać błędy podczas korzystania z mediów społecznościowych i to wpływa na nas.

Dodawanie jakiegokolwiek rodzaju kontaktu

- Bardzo częstym błędem w sieciach społecznościowych jest dodawanie wszelkiego rodzaju kontaktów. Może się to zdarzyć na takich platformach jak Facebook.
- Możliwe, że to co dodajemy jest botem, a nie prawdziwym użytkownikiem.
- Trzeba wiedzieć jak je rozróżnić i unikać dodawania każdego typu kontaktu, który otrzymuje zaproszenie.
- Czasami boty są zaprojektowane wyłącznie do zbierania danych o użytkownikach. Może to zagrozić naszej prywatności. Musimy mieć prawdziwy filtr na dodawane przez nas kontakty.
- Ważne jest, abyśmy wśród naszych znajomych mieli osoby, które nie stanowią problemu dla naszego bezpieczeństwa i prywatności.

Nie łącz się z sieciami społecznościowymi z dowolnego miejsca

- Pewnie często logujesz się poprzez sieci społecznościowe na dowolnej stronie. Jest to bardzo wygodne, ale nie najlepsze dla prywatności.
- Z pewnością przy wielu okazjach znajdujemy możliwość zarejestrowania się na stronie lub połączenia się z platformą poprzez Facebook lub Twitter. Unikamy rejestracji na tej stronie i wypełniania długiego formularza. Problem polega na tym, że za pośrednictwem Facebooka przekazujemy tej stronie dane osobowe. Te dane / informacje, które udostępniamy mogą być wykorzystane przez osoby trzecie w celach reklamowych.

Nie podawaj więcej informacji niż to konieczne

- Jest to zdecydowanie jeden z najgorszych nawyków, które posiada wielu użytkowników. Wprowadzają oni do sieci społecznościowych wiele danych osobowych, informacji, które tak naprawdę nie są niezbędne.
- Na przykład dane takie jak nasz numer telefonu, adres e-mail, informacje o miejscu zamieszkania .... Wszystko to wpływa na naszą reklamę i może być wykorzystane do złych celów.
- Nie podawaj więcej informacji niż jest to naprawdę konieczne. W ten sposób poprawimy naszą prywatność w sieci, a nawet możemy uniknąć pewnych problemów z bezpieczeństwem.

Rozpowszechnianie fałszywych wiadomości

- Problem fake newsów jest dziś wciąż aktualny. Mogę do nich dotrzeć wieloma drogami, ale bez wątpienia w sieciach społecznościowych są one bardziej niż obecne.
- Jak wiemy, to właśnie fake newsów używają jako przynęty, a czasem mogą nawet dystrybuować złośliwe oprogramowanie.
- Ważne jest, aby unikać dzielenia się tego typu fake newsami, a także uzyskać do nich dostęp, gdy widzimy je w mediach społecznościowych.

- Dzięki temu poprawi się nasze bezpieczeństwo.

Nie chronimy swojej prywatności

- Ostatnim błędem jest brak właściwej ochrony prywatności. Na przykład zostawiamy nasze profile otwarte, aby każdy mógł na nie wejść.
- Udostępniamy informacje każdemu, kto może je zebrać, aby stworzyć dla nas profil, a nawet wysyłać reklamy targetowane (wycelowane) lub przeprowadzać różne ataki, które wpływają na nasze bezpieczeństwo.

Inżynieria społeczna z perspektywy interdyscyplinarnej

- Ze względu na technikę stosowaną przez hakerów, konieczne jest podejście z perspektywy interdyscyplinarnej, takiej jak informatyka, psychologia, biznes i etyka.

Dyscyplina technologii informacyjnej

- Inżynieria społeczna powinna być omawiana w kontekście obecnych systemów informatycznych i ich obrony stosowanej jako forma ograniczania ryzyka.
- Uwierzytelnianie wieloczynnikowe jest powszechnym i często skutecznym sposobem potwierdzania przez organizacje, że osoba uzyskująca dostęp do systemów rzeczywiście powinna mieć ten dostęp
- Dodatkowym czynnikiem może być wykorzystanie wirtualnej sieci prywatnej (VPN), czyli uwierzytelnianie w celu dalszej walidacji użytkownika.

Dyscyplina psychologiczna

- Konieczne jest zrozumienie koncepcji i zrozumienie myśli i zachowań zarówno atakującego, jak i ofiary.
- Metody są ważne dla inżynierii społecznej, ponieważ są używane do obejścia zabezpieczeń, które mogą być w miejscu, takich jak zapory i systemy używane do identyfikacji intruzów.
- Pomaga zrozumieć działania pracowników, które są jedną z głównych przyczyn naruszeń danych.

Perspektywa biznesowa

- jest ważna, ponieważ inżynieria społeczna może dotyczyć wielu rodzajów przedsiębiorstw i mieć wpływ na to, jak organizacje są zorganizowane i zarządzane.
- pomaga określić czynniki, które wpływają na ataki inżynierii społecznej i jest korzystne, jeśli jest rozpatrywane w bardziej szczegółowych kategoriach w odniesieniu do następujących obszarów biznesowych: szkolenia i rozwój, udokumentowane polityki, procedury audytu wewnętrznego, budżety i kultura organizacyjna.
- może wykryć braki w każdym z tych obszarów, które mogą przyczynić się do ataków.

Perspektywa etyczna

- jest ważna w kontekście inżynierii społecznej i badań z nią związanych, ponieważ idea manipulowania innym człowiekiem narusza wiele zasad etycznych.
- pomaga, w przypadku zdarzenia z zakresu inżynierii społecznej, w leczeniu ofiar.

Ważne jest, aby uwzględnić:

- każdą dyscyplinę, dostarczając informacji o tym, jak rozumieć i interpretować temat, chronić się przed różnymi rodzajami ataków oraz rozumieć wpływ inżynierii społecznej zarówno z perspektywy ludzkiej, jak i organizacyjnej.
- że interpretacja tematu przez każdą dyscyplinę jest użyteczna tylko wtedy, gdy jest postrzegana w kontekście pozostałych dyscyplin.

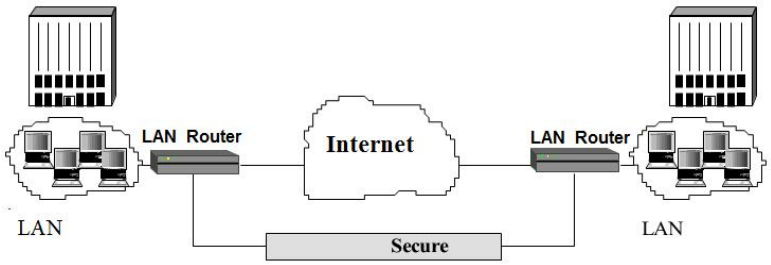
Techniki ochrony

- Inwentaryzacja sprzętu
- Inwentaryzacja aplikacji i systemów operacyjnych
- Kontrola urządzeń bezprzewodowych
- Projektowanie zabezpieczeń sieciowych
- Ograniczanie i kontrola portów sieciowych, protokołów komunikacyjnych i usług
- Ochrona obszarów peryferyjnych
- Fizyczny dostęp do lokalizacji
- Kontrolowane wykorzystanie uprawnień administracyjnych
- Monitorowanie i kontrola kont użytkowników
- Ocena umiejętności i szkolenia w zakresie bezpieczeństwa

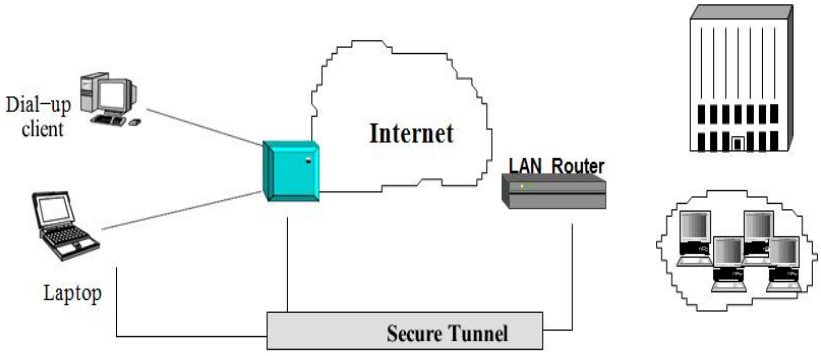
VPN – wirtualna sieć prywatna (ang. *Virtual Private Network*)

Wirtualna sieć prywatna to bezpieczne połączenie przez niezabezpieczoną sieć, taką jak Internet. Wirtualna oznacza istnienie unikalnej sieci, niezależnie od topologii, czyli grupy geograficznie rozproszonych komputerów, które komunikują się i mogą być administrowane jako jedna sieć.

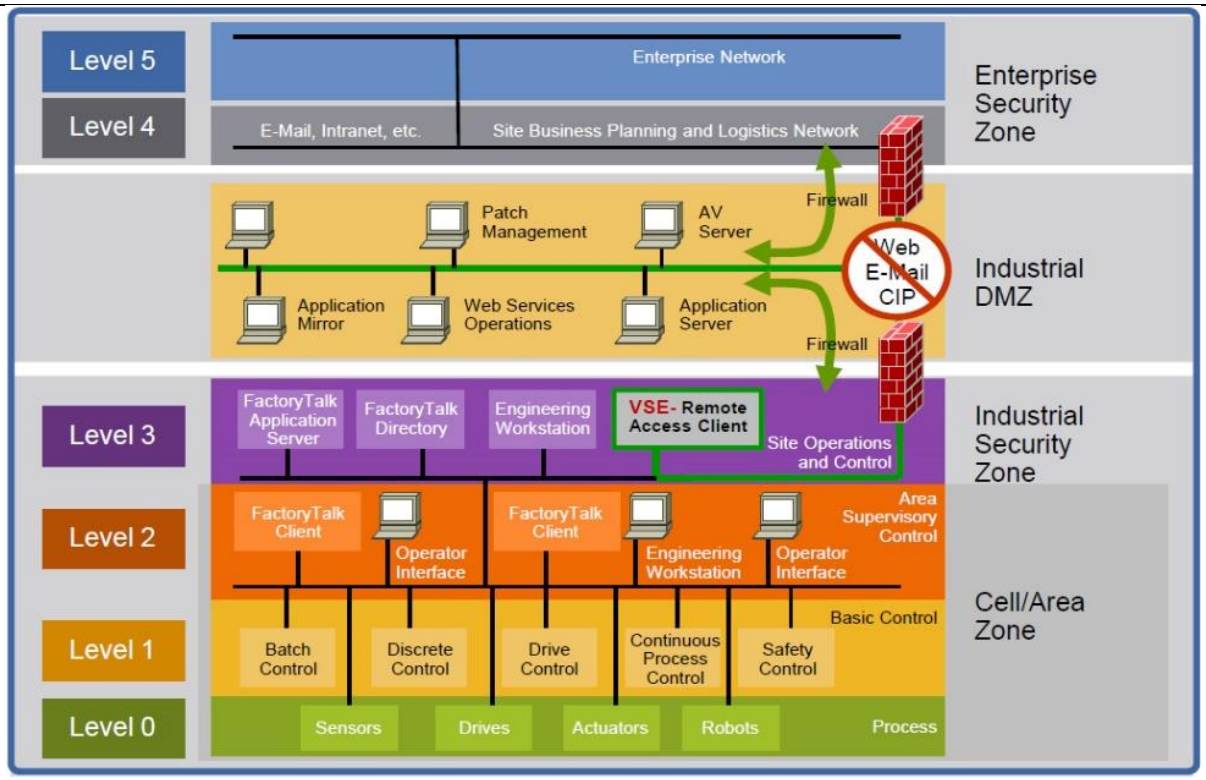
Prywatna oznacza sieć wirtualną z kontrolą dostępu. która zapewnia poufność, integralność wiadomości i uwierzytelnia pomiędzy użytkownikami i komputerami uczestniczącymi w komunikacji.



Rys. 2: VPN (wirtualna sieć prywatna)



Rys. 3: VPN dla zdalnego dostępu



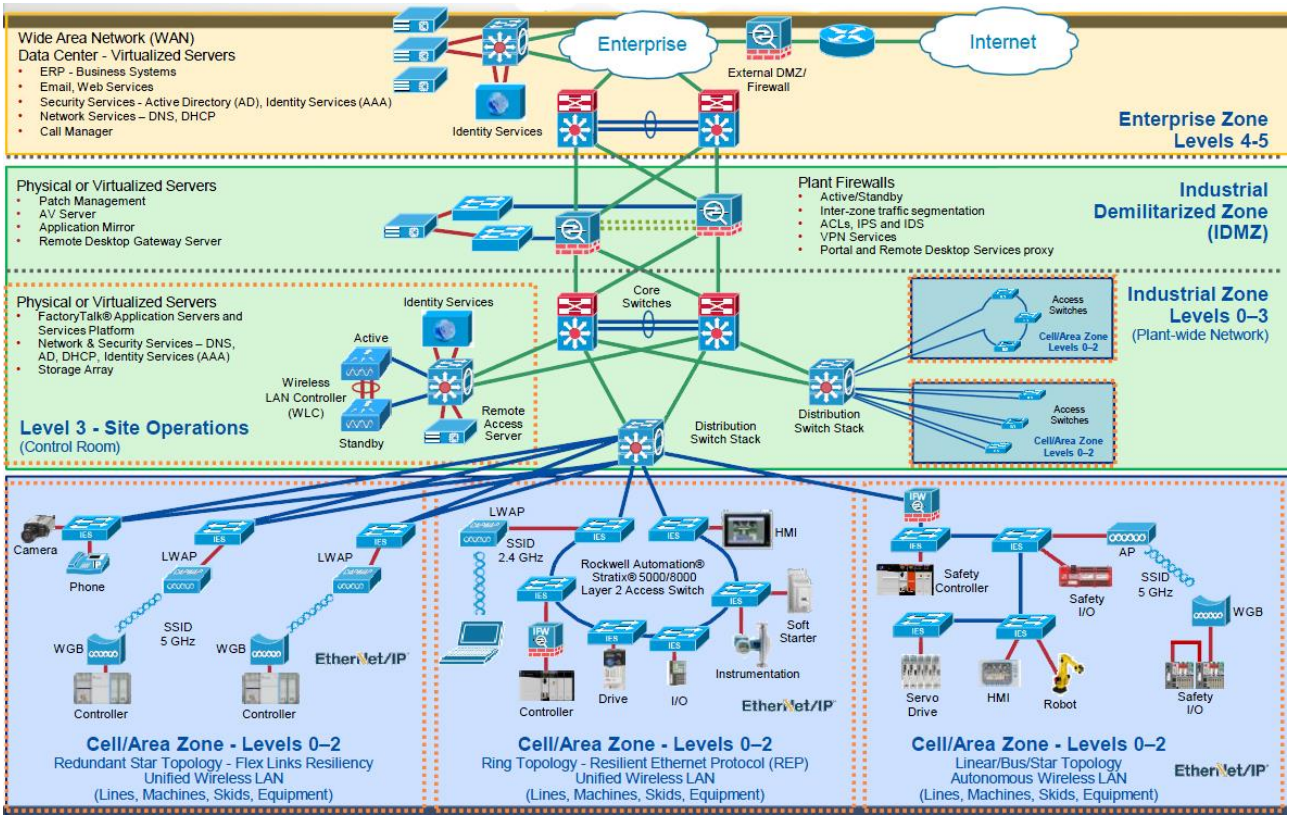
Rys. 4: Model logiczny ISA 95 - Przemysłowy system automatyki i sterowania (IACS)

- Obrona w głąb (DiD) wspiera to podejście. Opierając się na założeniu, że pojedynczy punkt ochrony może i prawdopodobnie zostanie pokonany, bezpieczeństwo DiD ustanawia wiele warstw ochrony poprzez połączenie zabezpieczeń fizycznych, elektronicznych i proceduralnych.
- Bank stosuje wiele środków bezpieczeństwa - takich jak kamery wideo, strażnik i skarbiec - co pomaga zapewnić, że zagrożenia napotkają więcej niż jedną linię obrony.
- Podejście "security-in-depth" obejmuje sześć głównych elementów:
    1. Polityki i Procedury
    2. Fizyczna
    3. Sieć
    4. Komputer
    5. Aplikacja
    6. Urządzenie

Tworzenie bezpiecznej infrastruktury przemysłowej

- Bezpieczeństwo fizyczne powinno ograniczać dostęp personelu nie tylko do obszarów obiektu, ale także do punktów wejścia do fizycznej infrastruktury sieciowej, takich jak panele sterowania, okablowanie i urządzenia.
- Segmentacja obszarów zakładu na wirtualne sieci lokalne (VLAN) jest najlepszą praktyką bezpieczeństwa w całej sieci.

- Mniejsze sieci VLAN są łatwiejsze do zarządzania i utrzymania w czasie rzeczywistym.
- Mogą one pomóc odizolować urządzenia od tych, które zostały naruszone, co pozwala utrzymać negatywny wpływ w obrębie jednej sieci VLAN.
- Jedną z omawianych technologii powinna być przemysłowa strefa zdemilitaryzowana (IDMZ), która tworzy krytyczną barierę ochronną między przedsiębiorstwem a obszarami przemysłowymi.
- IDMZ ogranicza ruch bezpośrednio pomiędzy tymi dwoma strefami i może pomóc w lepszym zarządzaniu dostępem poprzez wymuszanie uwierzytelniania lub monitorowanie ruchu pod kątem znanych zagrożeń.



Rys. 5: IDMZ

Pytania:

Pytania na forum dyskusyjnym, na które należy odpowiedzieć z krótkim uzasadnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentorskich

1. Jakie są zagrożenia w sieciach społecznościowych?
2. Środki zapewniające bezpieczeństwo i prywatność w sieciach społecznościowych
3. Jakie są główne techniki bezpieczeństwa w sieciach społecznościowych?

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

- Zagrożenia w sieciach społecznościowych
- Bezpieczeństwo i prywatność w sieciach społecznościowych
- Techniki bezpieczeństwa

Załączniki (Prezentacja PowerPoint, materiały informacyjne, wydruki, linki, wideo ...):
Zobacz załączniki

Referencje:

Wymagania dotyczące zamówień
URL: Procurement-requirements
URL: https://www.ekransystem.com/en/blog/third-party-providers
Określenie wymagań dotyczących zamówień
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Bezpieczeństwo i prywatność w sieciach społecznych
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Bezpieczeństwo i prywatność w sieciach społecznych
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Prywatność i bezpieczeństwo w internetowych mediach społecznościowych
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Techniki bezpieczeństwa danych i ochrona prywatności
URL: https://www.educba.com/data-security-techniques/
Czym są techniki bezpieczeństwa
URL: Security-concepts-developments-and-future-trends
Najskuteczniejsze techniki bezpieczeństwa
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/