Kerberos
OCHRONA INFORMACJI

Szkolenia

Informatyka – technologie
Informatyka - zarządzanie

Terminy i programy - styczeń, luty, marzec, kwiecień 2018

Wykładowcy

dr inż. Albert Sadowski, Kerberos OCHRONA INFORMACJI oraz Wyższa Szkoła Handlowa w Radomiu

dr inż. Tomasz Wasiak, Kerberos OCHRONA INFORMACJI oraz Politechnika Łódzka

Andrzej Dubis, Dyrektor Departamentu Informatyki, Podkarpacki BS w Sanoku

Roland Węgrzynowski, Kierownik Zespołu Teleinformatyki, Gospodarczy BS w Barlinku

Damian Nawrocki, Główny Specjalista ds. Strategii IT oraz Bezpieczeństwa Informatycznego, BS w Jastrzębiu Zdroju

Miejsca szkoleń, koszt

Instytut Biocybernetyki Polskiej Akademii Nauk, Warszawa, ul. Trojdena 4

Wyższa Szkoła Handlowa w Radomiu (opcja dodatkowa)

Godziny szkoleń: 10 – 15

Koszt: 490 zł + VAT (23%)

Informacje, zgłoszenia

Katarzyna Wiśniewska, Koordynator Szkoleń i Konferencji
kom. 609 115 192, katarzyna.wisniewska@kerberos.pl

Kerberos
OCHRONA INFORMACJI

Terminy

Informatyka – technologie

Kod	Tytuł	Styczeń 2018	Luty 2018	Marzec 2018	Kwiecień 2018
BBI	**Bezpieczeństwo Bankowości Internetowej**			14	
BSI	**Bezpieczeństwo Systemów Informatycznych**	30			20
FWVPN	**Systemy firewall i VPN**	23		6	
TSB	**Technologie sieciowe i bezpieczeństwo sieci komputerowych**	26		28	
WOK	**Wprowadzenie do ochrony informacji i kryptografii**		8		25
TAB	**Przeprowadzanie testów penetracyjnych w niewielkich sieciach heterogenicznych – warsztaty**	24		13	
USL	**Podstawy używania środowiska linux na serwerach – warsztaty**				10
ZSW	**Zabezpieczanie systemów Windows – warsztaty**		15		19
ZSL	**Zabezpieczanie systemów Linux – warsztaty**		23	23	

Informatyka – zarządzanie

Kod	Tytuł	Styczeń 2018	Luty 2018	Marzec 2018	Kwiecień 2018
PAB	**Przygotowanie Banku do Audytu Bezpieczeństwa**				12
PRD	**Przygotowanie Banku do inspekcji dot. Rekomendacji D**	18			17
WDIT	**Warsztaty tworzenia bankowej dokumentacji IT zgodnej z Rek.**			1	
ZPR	**Zarządzanie projektami IT**		7	7	
ITMAN	**Informatyka w zarządzaniu Bankiem – dla managerów**	31		8	
WPB	**Warsztaty tworzenia dokumentacji polityki bezpieczeństwa**		13		4
RBP	**Rekomendacja KNF dot. bezpieczeństwa płatności internetowych**		14	15	
ZOI	**Zarządzanie obszarem informatyki w Banku**		20	9	
PSD	**Wdrożenie dyrektywy PSD2 w systemach bankowości internetowej**	19		21	
ZRIT	**Zarządzanie ryzykiem IT w Banku**	25		27	
KABI	**Kurs ABI / IOD**		21		11
WABI	**Warsztaty tworzenia dokumentacji ODO – dla ABI / IOD**		27	22	
ZIB	**Zagadnienia informatyczne w Banku – dla managerów i nie-informatyków**		22		24
WPCD	**Warsztaty tworzenia Planów Ciągłości Działania**		6	20	

Kerberos
OCHRONA INFORMACJI

Programy

Informatyka – technologie

Informatyka – zarządzanie

Kerberos
OCHRONA INFORMACJI

Kod: **BBI**

Tytuł: **Bezpieczeństwo Bankowości Internetowej**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Podczas szkolenia omówione będą następujące zagadnienia:

- metody ataków na systemy Bankowości Internetowej,
- stosowane techniki zabezpieczeń,
- rekomendacja Komisji Nadzoru Finansowego dotycząca bezpieczeństwa płatności internetowych.

Program

Ataki na systemy Bankowości Internetowej

Współczesna Bankowość Internetowa – rys historyczny, stan obecny

Najczęstsze typy ataków

Metody ochrony przed atakami

Jaka ochrona jest najlepsza?

Największe zagrożenia – teraz i w najbliższej przyszłości.

Jak zabezpieczane są Banki Internetowe?

Zabezpieczenia infrastrukturalne
Szyfrowane sesje SSL
Certyfikaty i infrastruktura klucza publicznego
Klucze prywatne, klucze publiczne
Metody uwierzytelniania klienta Banku Internetowego
Idea haseł / kodów jednorazowych (twierdzenie Lamporta)
Protokoły typu *challenge – response*
Podpis cyfrowy
Zastosowanie kart inteligentnych / tokenów
Rodzaje tokenów

Rekomendacja KNF dotycząca bezpieczeństwa płatności internetowych

Omówienie i ocena Rekomendacji
Wskazanie najbardziej problematycznych punktów
Co już jest wdrożone?
Co powinien zrobić Bank, by wdrożyć Rekomendację?
Co powinni zrobić dostawcy systemów bankowości internetowej, by wdrożyć Rekomendację?

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych. Udział w niej nie wymaga żadnej dodatkowej opłaty.

Kerberos
OCHRONA INFORMACJI

Kod: **KABI**

Tytuł: **Kurs ABI/IOD**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

- Szkolenie przeznaczone jest dla osób pełniących, bądź przygotowujących się do pełnienia funkcji Administratora Bezpieczeństwa Informacji / Inspektora Ochrony Danych (ABI/IOD) w organizacji.
- Szkolenie **nie wymaga dogłębnej znajomości zagadnień informatycznych**, przeznaczone jest zarówno dla informatyków, jak i przedstawicieli innych specjalności (Głównych Księgowych, członków zarządów, specjalistów ds. ryzyk, audytorów itp.).
- Celem szkolenia jest wyposażenie słuchaczy w komplet wiedzy i umiejętności niezbędnych do pełnienia funkcji ABI/IOD w organizacji.
- Ukończenie kursu potwierdzone jest wystawieniem „**Certyfikatu ABI/IOD**".

Program

- Ustawa o ochronie danych osobowych i rozporządzenia wykonawcze.
- RODO – czyli ostatnia, unijna nowelizacja przepisów dot. ochrony danych osobowych.
- Jakie zmiany wprowadza RODO?
- Implementacja RODO na gruncie polskim; nowelizacja polskiego prawa wynikająca z RODO.
- Rola ABI/IOD w organizacji.
- Dlaczego *per saldo* warto zgłosić ABI/IOD do GIODO?
- Generalny Inspektor Ochrony Danych Osobowych i inspekcje.
- Zasady przetwarzania danych osobowych, prawa osoby, której dane dotyczą.
- Zabezpieczenie danych osobowych, rejestracja zbiorów danych osobowych.
- Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych […].
- Zgłoszenie ABI/IOD do GIODO.
- Prowadzenie rejestru zbiorów danych osobowych.
- Sprawdzenia (auto-inspekcje).
- Wymogi formalne i dokumentacyjne nakładane przez ustawodawcę na Administratora Danych.
- Funkcje kontrolne realizowane przez ABI, współpraca z działem informatyki i zarządem Banku.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we wwłasnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **WABI**

Tytuł: **Warsztaty tworzenia dokumentaji ODO – dla ABI/IOD**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

- Szkolenie przeznaczone jest dla osób pełniących, bądź przygotowujących się do pełnienia funkcji Administratora Bezpieczeństwa Informacji (ABI) w Banku Spółdzielczym. Jest uzupełnieniem / rozszerzeniem szkolenia „Kurs ABI/IOD".
- Szkolenie **nie wymaga dogłębnej znajomości zagadnień informatycznych**, przeznaczone jest zarówno dla informatyków, jak i przedstawicieli innych specjalności (Głównych Księgowych, członków zarządów, specjalistów ds. ryzyk, audytorów itp.).
- Szkolenie ma formę **warsztatów**; uczestnicy ćwiczą praktyczną umiejętności pisania / aktualizowania dokumetacji związanej z ochroną informacji.
- Ukończenie kursu potwierdzone jest wystawieniem certyfikatu.

Program

- Teoretyczne podstawy bezpieczeństwa informacji i ochrony danych osobowych.
- Jaka dokumentacja jest wymagana przez Ustawę o ochronie danych osobowych i rozporządzenia wykonawcze?
- Jak tworzyć dokumentację wymaganą przepisami, by nie była zbyt obszerna, a jednocześnie zawierała wszystkie konieczne informacje?
- Warsztaty projektowe – tworzenie dokumentu Polityki Bezpieczeństwa.
- Warsztaty projektowe – tworzenie dokumentu wykonawczego - Instrukcji Bezpieczeństwa.
- Warsztaty projektowe – tworzenie ewidencji i opisów wymaganych przez Ustawę i rozporządzenie wykonawcze.
- Plany Ciągłości Działania – zasady tworzenia użytecznej dokumentacji.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **PAB**

Tytuł: **Przygotowanie Banku Spółdzielczego do Audytu Bezpieczeństwa**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

I. Przygotowanie do audytu dokumentacji i procedur polityki bezpieczeństwa

Zarządzanie kontami, identyfikatorami i hasłami użytkowników, Rozpoczynanie i kończenie pracy w systemie, Tworzenie i przechowywanie wydruków i kopii bezpieczeństwa, Metody ochrony przed wirusami, Przeglądy, naprawy i likwidacja sprzętu i nośników, Zasady bezpiecznego użytkowania sieci komputerowych, Procedury ograniczania dostępu fizycznego osobom nie mającym prawa do pracy w systemie, Kontrola mechanizmów, procedur, oprogramowania i sprzętu służących do zabezpieczania danych, Utrzymanie ciągłości działania, Plany Ciągłości Działania, postępowanie w przypadku. naruszenia bezpieczeństwa.

II. Przygotowanie do audytu ochrony danych osobowych

Audyt dokumentacji wymaganej Ustawą o ochronie danych osobowych oraz aktami wykonawczymi do Ustawy, wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych, wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami, określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, ewidencja osób upoważnionych do przetwarzania danych osobowych (wymóg ustawowy), pisemne upoważnienia na przetwarzanie danych osobowych (wymóg ustawowy), pisemne zobowiązania osób przetwarzających dane osobowe, wymagania dotyczące aplikacji służących do przetwarzania danych osobowych.

III. Audyt technicznych aspektów zabezpieczeń

Audyt serwera głównej aplikacji bankowej, audyt serwera zapasowego, audyt serwera bankowości internetowej, audyt serwera obsługi kart, audyt serwerów WWW, poczty, audyt serwerów komunikacyjnych (z systemami u outsourcerów), audyt urządzeń sieciowych: routerów, firewalli, bramek VPN, systemów IDS/IPS, zarządzalnych *switchy,* Audyt baz danych.

IV. Testy penetracyjne z Internetu

Istota testów penetracyjnych z Internetu (symulacji włamań), przygotowanie do testów.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kod: **PRD**

Tytuł: **Przygotowanie Banku do inspekcji KNF dot. Rekomendacji D**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Celem szkolenia jest dostarczenie słuchaczom wiedzy niezbędnej do poprawnego przygotowania Banku do inspekcji KNF dotyczącej Rekomendacji D.

- SIZ – typowe błędy i sposoby ich korygowania.
- Strategia w zakresie technologii informatycznej – typowe błędy i sposoby ich korygowania
- Zasady współpracy biznesu i IT – czy i kiedy nadawać im postać formalną?
- Wykaz obowiązków i uprawnień w kontekście relacji ABI – ASI – Szef IT.
- Wykaz właścicieli poszczególnych systemów – jak poprawnie rozumieć pojęcie „właściciela systemu”?
- Wykaz kluczowych pracowników obszarów technologii – jakich informacji brakuje w BS-ach?
- Zasady prowadzenia projektów – dlaczego podejście minimalistyczne jest wystarczające?
- Dokumentacja procesu zarządzania zmianą – jakie braki występują w BS-ach?
- Spis inwentaryzacyjny przetwarzanych danych – kiedy jest sens klasyfikacji danych?
- Zasady zarządzania jakością danych – co tu można zrobić?
- Zasady współpracy z zewn. dostawcami usługodawców – co jeszcze można poprawić?
- PCD jako jeden z najsłabszych punktów BS-ów – jak tworzyć poprawne PCD i procedury awaryjne?
- Bezpieczeństwo IT – typowe niedociągnięcia w BS-ach i jak je eliminować?
- Audyty bezpieczeństwa w BS-ach – rola audytu wewnętrznego i zewnętrznego.
- Ogólna ocena poziomu kultury informatycznej Banków Spółdzielczych vs stan dokumentacyjny.
- „Nadwaga biurokratyczna” obszarów IT Banków Spółdzielczych i jak z nią walczyć?
- Wypaczanie zasady proporcjonalności przez firmy informatyczne.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **WDIT**

Tytuł: **Warsztaty tworzenia bankowej dokumentacji IT zgodnej z Rekomendacją D**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Szkolenie ma formę warsztatową. W ramach praktycznych ćwiczeń, Słuchacze – przy wsparciu Wykładowcy – tworzą dokumentację IT (wymaganą przez Rekomendację D), dopasowaną do potrzeb własnego Banku.

Jednym z celów szkolenia jest wskazanie, jak można sobie radzić z „nadwagą biurokratyczną" obszarów IT Banków Spółdzielczych i jak stworzyć, krótką, zwięzłą, a jednocześnie rzeczową i użyteczną dokumentację dla własnego Banku.

Warsztaty obejmują tworzenie dokumentacji, dotyczącej następujących obszarów tematycznych:

- SIZ w obszarze informatyki i bezpieczeństwa IT
- Strategia w zakresie technologii informatycznej
- Zasady współpracy biznesu i IT
- Obowiązki i uprawnienia dla stanowisk związanych z obszarem IT
- Wykaz systemów, ich kwalifikacja, wykaz właścicieli poszczególnych systemów
- Wykaz kluczowych pracowników obszarów technologii
- Zasady prowadzenia projektów
- Dokumentacja procesu zarządzania zmianą
- Spis inwentaryzacyjny przetwarzanych danych, klasyfikacja danych
- Zasady zarządzania jakością danych
- Zasady współpracy z zewn. dostawcami usługodawców
- Plany Ciągłości Działania (PCD)
- Polityka bezpieczeństwa i instrukcje wykonawcze
- Audyty bezpieczeństwa - wewnętrzne i zewnętrzne

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZPR**

Tytuł: **Zarządzanie projektami IT**

Liczba dni: **1**

Wykładowca: **Andrzej Dubis, Podkarpacki BS w Sanoku**

Program

I. Przygotowanie do rozpoczęcia Projektu w firmie – właściciel, sponsor, podział odpowiedzialności

Jak określić potrzeby i przejść do wykonania zgodnie z potrzebami organizacji. Kto powinien uczestniczyć w Projekcie aby zakończył się sukcesem w określonym budżecie i wymaganym czasie. Odpowiedzialność członków Zespołu i podział prac.

Dobranie uczestników w zależności od skali Projektu i ich umiejscowienia w firmie. Jak pogodzić sprzeczność między pracą w Zespole a codziennymi obowiązkami w swoim miejscu pracy.

II. Jak zminimalizować ryzyko w Projekcie? – identyfikacja i uprzedzanie kłopotów

Plany zarządzania ryzykiem projektowym w oparciu o modele i strategie. Co zrobić by efektywnie minimalizować ryzyko. Jak to naprawdę wygląda w świecie rzeczywistym.

III. Czy Biuro Projektów jest niezbędne w organizacji?

Czy trzeba stworzyć Biuro aby osiągnąć mierzalne efekty. Jakie uprawnienia nadać aby mogło realizować sprawnie powierzone zadania. Stałe Biuro Projektów czy tylko dopóki istnieją Projekty?

IV. Czy Biuro Projektów jest niezbędne w organizacji?

Czy trzeba stworzyć Biuro aby osiągnąć mierzalne efekty. Jakie uprawnienia nadać aby mogło realizować sprawnie powierzone zadania. Stałe Biuro Projektów czy tylko dopóki istnieją Projekty?

V. Zarządzanie Zespołem w Projekcie

Jakie kompetencje techniczne czy nie techniczne uwzględnić kompletując Zespół. Komunikacja w grupie i motywacja jako narzędzia do utrzymania pełnego zaangażowania uczestników Projektu na poszczególnych etapach prac. Narzędzia zarządzania Projektami w zależności od stopnia złożoności Projektu oraz skali organizacji.

VI. Case study

Przykład realizacji Projektu od kick off do zamknięcia Projektu. Omówienie poszczególnych etapów na realnym przykładzie, pokazującym bieżące problemy oraz sposoby ich rozwiązania.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZIB**

Tytuł: **Zagadnienia informatyczne w Banku – dla mangerów i nie-informatyków**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Szkolenie ma formę wykładu elementarnego; przeznaczone jest dla osób, które nie mają wykształcenia informatycznego, ale których obowiązki służbowe wymagają rozumienia podstawowych pojęć i zagadnień dotyczących obszaru informatyki w Banku.

Odbiorcami szkolenia są:

- Główni Księgowi, Prezesi i Członkowie Zarządów,
- Specjaliści ds. ryzyk,
- Specjaliści ds. audytów wewnętrznych i kontroli,
- Administratorzy Bezpieczeństwa Informacji / Inspektorzy Ochrony Danych,
- Dyrektorzy komórek, oddziałów, managerowie
- przedstawiciele innych, **nie-informatycznych,** specjalności.

Podstawy ochrony informacji	• Poufność i autentyczność informacji • Szyfrowanie, rodzaje szyfrów • Podpis cyfrowy • Infrastruktura klucza publicznego • Certyfikaty, Centra certyfikacji
Podstawy działania sieci lokalnych i internetu. Bezpieczenstwo komunikacji sieciowej.	• Jak działają sieci lokale? • Urządzenia sieci lokalnych: switch, switch zarządzalny • Segmentacja sieci (VLAN-y) • Architektura i sposób działania Internetu, adresacja IP • Protokoły komunikacji internetowej • Wirtualne sieci prywatne (VPN) • Urządzenia sieci rozległych: router / firewall / bramka VPN • Zapezpieczanie komunikacji internetowej – architektury i sposób działania systemów firewall, funkcje dodatkowe • Systemy detekcji intruzów (IDS/IPS)
Podstawy uwierzytelniania	• Logowanie się do systemów • Hasła stałe • Koncepcja haseł jednokrotnych • Protokoły *challange - response* • Procedura Laporta • Wykorzystanie tokenów w uwierzytelnianiu
Systemy operacyjne i aplikacje	• Systemy operacyjne; rodzaje i architektury • Bazy danych • Architektura aplikacji, model klient- serwer • Wirtualizacja środowisk informatycznych • Logowanie, kopie zapasowe, ochrona antywirusowa • Bezpieczeństwo aplikacji
Podstawy bezpieczenstwa Bankowości Internetowej	• Zabezpieczenia infrastrukturalne • Szyfrowane sesje SSL

	• Certyfikaty i infrastruktura klucza publicznego • Klucze prywatne, klucze publiczne • Metody uwierzytelniania klienta Banku Internetowego • Idea haseł / kodów jednorazowych (twierdzenie Lamporta) • Metody dystrybucji i generowania haseł / kodów jednorazowych (karty, SMS, tokeny) • Protokoły typu *challenge – response* w BI • Zastosowanie kart inteligentnych / tokenów • Rodzaje tokenów

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ITMAN**

Tytuł: **Informatyka w zarządzaniu Bankiem – dla managerów**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

- Modele funkcjonowania systemów core'owych Banku: w siedzibie Banku, w zrzeszeniu, w firmie outsourcingowej. Wady i zalety poszczególnych modeli. Zagrożenia i korzyści związane z centralizacją oraz outsourcingiem systemu core'owego (wyniki badań naukowych).
- Systemy towarzyszące – modele użytkowania.
- Wybór rozwiązań IT – zakupy rozwązań budżetowych vs. zakupy rozwiązań „markowych". Rożnice faktycznie między różnymi kategoriami cenowymi rozwiązań IT.
- Mit niedoinwestowania Banków Spółdzielczych w obszarze IT. Beneficjenci tego mitu.
- Czy funkcjowalność systemów IT w Bankach Spółdzielczych istotnie różni się od funkcjonalności w systemów w Bankach komercyjnych.
- Rola zrzeszeń w zakupach i wdrażaniu systemów IT. Stosunek informatyków do propozycji zrzeszeń (wyniki badań naukowych). Współpraca służb IT Banków Spółdzielczych z departamentami IT zrzeszeń (wyniki badań). Zakupy systemów i rozwiązań IT – indywidualne w Bankach Spółdzieczych vs. globalne, za pośrednictwem Banków Zrzeszających (wyniki badań).
- Specyfika i struktura służb IT w Banku Spółdzielczym. Modele funkcjonowania komórek IT w Bankach Spółdzielczych. Liczebność perosonelu IT.
- Ochrona danych osobowych w Bankach Spółdzielczych. Modele funkcjonowania funkcji ABI w Bankach Spółdzielczych.
- Wsparcie formalno – dokumentacyjne zrzeszeń w zakresie obszaru IT i wymogów Rekomendacji D. Biurkratyzacja obszarów IT wynikła z działań wspierających ze strony zrzeszeń.
- Relizacja projektów informatycznych w Bankach Spółdzielczych.
- Realizacji projektów IT globalnych (zrzeszeniowych) w ocenie bankowych informatyków.
- Strategia IT w Bankach Spółdzielczych – jak ją racjonalnie budować.
- Dokumentacja i formalizm dotyczacy obszaru informatyki.
- Zarządzanie jakością danych, zarządzanie systemami informatycznymi.
- Audyt IT wewnętrzne i zewnętrzne w Bankach Spółdzielczych.
- Relacje zarząd – komórka informatyczna w Banku Spółdzielczym (wyniki badań).
- Bankowość Internetowa w Bankach Spółdzielczych – modele, zagrożenia, zalecane mechanizmy bezpieczeństwa. Wizja wdrożenia dyrektywy unijnej PSD2.
- Korzystanie przez Banki Spółdzielcze z centrów bezpieczeństwa (typu CERT)

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kod: **BSI**

Tytuł: **Bezpieczeństwo systemów informatycznych**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Polityka i strategie bezpieczeństwa
- Zagrożenia i przedmioty ochrony.
- Dokument polityki bezpieczeństwa.
- Instrukcje wykonawcze do polityki bezpieczeństwa
- Aspekt ludzki w ochronie informacji.

Bezpieczna wymiana informacji w sieciach komputerowych - wprowadzenie.
- Protokoły bezpiecznej komunikacji.

Techniki kontroli dostępu do systemu komputerowego.
- Wprowadzenie.
- Ustalone hasła.
- Współdzielony klucz.
- Identyfikacja użytkownika w kryptografii z kluczem jawnym.
- Identyfikacja obustronna w kryptografii z kluczem jawnym.
- Procedura Lamporta.
- Implementacje z wykorzystaniem inteligentnych kart.
- Bilety.
- Konstruowanie bezpiecznych protokołów uwierzytelniania.

Bezpieczeństwo systemu operacyjnego.
- Bezpieczeństwo systemów wolnostojących, dostęp do systemu, dostęp do zasobów systemu.
- Systemy pracujące w sieci.
- Podsumowanie.

System uwierzytelniania Kerberos.
- Wprowadzenie.
- Protokół Kerberos.
- Wady i ograniczenia protokołu Kerberos.

Systemy zaporowe.
- Podstawowe informacje o systemach zaporowych.
- Rodzaje architektur sieciowych systemów zaporowych.
- Komputery typu bastion host.
- Prezentacja przykładowego systemu firewall.

Testowanie i monitorowanie poziomu bezpieczeństwa.
- Przegląd zadań wykonywanych przez programy testujące poziom bezpieczeństwa (skanery bezpieczeństwa):
- Aktywna ochrona systemów i sieci: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS).
- Prezentacja przykładowego skanera bezpieczeństwa.

Bezpieczeństwo protokołu IP.
- IPSec, IPv6.
- Tryby pracy dla protokołu IPSec.
- Protokół SKIP.
- Dystrybucja kluczy sesyjnych.
- Wirtualne Sieci Prywatne.
- Prezentacja przykładowego rozwiązania VPN.

Ataki na systemy.
- DoS, IP spoofing, DNS spoofing, spamming, crack, SYN flooding, buffer overflow, konie trojańskie, ataki z wykorzystaniem WWW.
- Ochrona przed atakami, systemy automatyczne.
- Współpraca systemów zaporowych systemów systemami IDS.

Kryptografia i i techniki kryptograficzne.
- Ochrona poufności, ochrona autentyczności wiadomości i nadawcy.
- Szyfrowanie, deszyfracja.

- Kryptosystemy symetryczne i asymetryczne.
- Podpisy cyfrowe.

Infrastruktura klucza publicznego.

- Problem bezpiecznej komunikacji w sieciach.
- Klucz sesyjny; uzgadnianie i dystrybucja, procedura Diffiego-Hellmana.
- Klucze publiczne i ich certyfikaty.
- Urzędy ds. Certyfikatów.
- Zastosowania: SSH, PGP.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **WPB**

Tytuł: **Warsztaty tworzenia dokumentacji polityki bezpieczeństwa**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Szkolenie ma formę warsztatową. W ramach praktycznych ćwiczeń, Słuchacze – przy wsparciu Wykładowcy – tworzą dokumentację polityki bezpieczeństwa (wraz z instrukcjami wykonawczymi), dopasowaną do potrzeb własnego Banku.

Jednym z celów szkolenia jest wskazanie, jak można sobie radzić z „nadwagą biurokratyczną" obszarów IT Banków Spółdzielczych i jak stworzyć, krótką, zwięzłą, a jednocześnie rzeczową i użyteczną dokumentację dotyczącą bezpieczeństwa (polityka i instrukcje wykonawcze) dla własnego Banku.

- Warsztaty obejmują tworzenie dokumentacji, dotyczącej następujących obszarów tematycznych:
- Zarządzanie kontami, identyfikatorami i hasłami użytkowników,
- Rozpoczynanie i kończenie pracy w systemie,
- Tworzenie i przechowywanie wydruków i kopii bezpieczeństwa,
- Metody ochrony przed wirusami, Przeglądy, naprawy i likwidacja sprzętu i nośników,
- Zasady bezpiecznego użytkowania sieci komputerowych,
- Procedury ograniczania dostępu fizycznego osobom nie mającym prawa do pracy w systemie,
- Kontrola mechanizmów, procedur, oprogramowania i sprzętu służących do zabezpieczania danych,
- Utrzymanie ciągłości działania, Plany Ciągłości Działania,
- Postępowanie w przypadku. naruszenia bezpieczeństwa,
- Audyty bezpieczenstwa wewnętrzne i zewnętrzne.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kod: **FWVPN**

Tytuł: **Systemy firewall i VPN**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Szkolenie ma formę wykładowo – projektową. W ramach szkolenia prowadzone będą:

- Wykłady teoretyczne
- Ćwiczenia projektowe, polegające na samodzielnym wykonywaniu przez uczestników szkolenia projektów:

- architektur systemów zaporowych,
- reguł filtracji ruchu,
- reguł translacji adresów sieciowych.

I. Wykład

1. Techniki kontroli przesyłanych informacji.
   - Sposoby działania systemów zaporowych; podział na filtry pakietowe, gateway-e poziomu aplikacji oraz opis techniki stateful inspection.
   - Wykorzystanie techniki stateful inspection do kontrolowania połączeń dla protokołów bezpołączeniowych (np. RPC, UDP).
2. Architektury systemów zaporowych.
3. Architektury implementacji systemów zaporowych.
   - Systemy jednowęzłowe, systemy rozproszone z oddzielonymi punktami kontroli pakietów (punktami inspekcyjnymi) od punktów zarządzania.
   - Systemy centralnego zarządzania punktami inspekcyjnymi, możliwość zarządzania listami dostępowymi routerów.
   - Bezpieczna komunikacja pomiędzy komponentami rozproszonego systemu systemu zaporowego.
4. Graficzne systemy zarządzania zaporami ogniowymi.
   - Edytory reguł zabezpieczeń działające w systemach 'okienkowych'.
   - Definicja obiektów typu komputery, gateway-e, sieci, przestrzenie adresowe, routery, użytkownicy, grupy użytkowników.
5. Użytkownicy i uwierzytelnianie.
   - Użytkownicy i grupy użytkowników.
   - Techniki uwierzytelniania: uwierzytelnianie użytkowników, komputerów, uwierzytelniane specyficzne dla aplikacji. Tryby uwierzytelniania: przeźroczyste i nieprzeźroczyste.
   - Algorytmy uwierzytelniania: hasła systemu, hasła zapory ogniowej, hasła jednokrotne, karty inteligentne, zewnętrzne serwery uwierzytelniające.
6. Serwery proxy i kontrola zawartości (content security).
   - Rola serwerów proxy.
   - Content security - przykłady dla protokołów HTTP, SMTP, FTP, kontrola antywirusowa (dedykowane serwery).
7. NAT - translacja adresów sieciowych.
   - Idea translacji, zalety, ograniczenia.
   - Techniki translacji: statyczna i dynamiczna, tryby translacji dynamicznej: many-to-one, many-to-many, priorytety przyznawania adresów IP.
8. Techniki równoważenia obciążenia serwerów wewnątrzsieciowych.
   - Idea rozwiązania, uzasadnienie potrzeby stosowania równoważenia obciążenia.
   - Algorytmy równoważenia obciążenia: server load measure, round trip, round robin, algorytm losowy.
9. Wirtualne Sieci Prywatne.
   - Idea: systemy klucza publicznego, procedura Diffiego-Hellmana, podpisy cyfrowe, urzędy ds. certyfikatów.
   - Algorytmy VPN: SKIP, IPSec, IKE.
   - Stosowane algorytmy szyfrowania (DES, RC4, RC5, Triple-DES, propozycje AES) i podpisów cyfrowych (RSA,MD5, techniki MAC).
10. Rejestrowanie ruchu przechodzącego przez zaporę ogniową.
    - Systemy rejestrowania, pliki typu log.

- Statystyki wychodzących i wchodzących połączeń, rozliczanie użytkowników, badanie obciążenia serwerów wewnątrzsieciowych.
- Monitorowanie aktywnych sesji sieciowych. Analiza zajętości pasma przez poszczególne usługi, aplikacje, użytkowników itp.

II.Ćwiczenia projektowe.

Uczestnicy szkolenia wykonują serię pisemnych ćwiczeń w celu uzyskania biegłości w projektowaniu architektur systemów zaporowych, tworzenia reguł filtracji ruchu sieciowego, reguł translacji statycznej i dynamicznej adresów.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **TSB**

Tytuł: **Technologie sieciowe i bezpieczeństwo sieci komputerowych**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Architektura sieci

- Sieci lokalne (LAN) a sieci rozległe (WAN)
- Idea adresacji w sieciach rozległych, podział sieci rozległej na segmenty
- Routing i tablice routingu, segmentacja sieci
- Adresy logiczne (IP), adresy sprzętowe (MAC), konwersja adresów
- Architektura warstwowa, 7-warstowy model referencyjny, 4-warstwowy model referencyjny TCP/IP
- Architektury aplikacji sieciowych: klient – serwer, architektura peer-to-peer, architektura mieszana

Protokól internetowy IP

- Struktura pakietu IP
- Nagłówki Ipv4 i Ipv6

Protokoły warstwy transportu – TCP i UDP

- Podstawowe różnice między protokołami TCP i UDP, zastosowania tych protokołów
- Nagłówek TCP
- Ustanawianie i kończenie połączenia TCP
- Nagłówek UDP

Protokół ARP

- Koncepcja ARP, RARP
- Lokalizacja ARP w modelu referencyjnym
- Zasady działania protokołu ARP
- Struktura pakietu ARP
- Przykład: działanie protokołu ARP w kontekście sieci rozległej
- Tablica ARP Cache

Sieci Ethernet i Wifi, urządzenia sieciowe

- Sieci galaniczne Ethernet
- Format ramki ethernetowej
- Protokół CSMA/CD
- Hub (koncentrator) – zasada działania, warstwa działania
- Switch (przełącznik) – koncepcja przełączania
- Tablica switcha (switch table)
- Porównanie funkcji huba, switcha i routera; warstwy działania
- Sieci bezprzewodowe
- Bezpieczeństwo sieci bezprzewodowych

Protokół ICMP

- Zastosowanie protokołu ICMP
- Warstwa działania
- Komunikaty o błędach (error reporting) i ich typy
- Komunikaty informacyjne (query messages)
- Struktura komunikatów ICMP
- Zastosowanie protokołu ICMP: ping, traceroute

System DHCP i autokonfiguracja

- Zastosowanie protokołu DHCP
- Ręczne a dynamiczne przypisanie adresu
- Sekwencja komunikatów w DHCP
- Wiele serwerów DHCP w sieci
- Jeden serwer DHCP – wiele zapytań; rozróżnianie zapytań
- Wygaszanie i odnawianie dzierżawy adresu

System nazw domenowych DNS
Systemy firewall, Translacja adresów sieciowych (NAT),
Sieci VPN
Protokóły bezpiecznej komunikacj sieciowej
Bezpieczna komunikacja w oparciu o SSL/TLS
Ataki na sieci komputerowe
Polityka bezpieczeństwa sieci

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kod: **WOK**

Tytuł: **Wprowadzenie do ochrony informacji i kryptografii**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Wprowadzenie - pojęcia i koncepcje ogólne

- Ochrona poufności
- Ochrona autentyczności
- Tekst jawny, szyfrogram, przekształcenie szyfrujące
- Alfabet tekstu jawnego, alfabet szyfrogramu
- Przestrzeń tekstu jawnego, przestrzeń szyfrogramu
- Szyfrowanie, deszyfrowanie, kryptosystem
- Szyfry monoalfabetyczne i polialfabetyczne

Kryptografia symetryczna a kryptografii asymetryczna

- Koncepcja kryptrografii symetrycznej
- Koncepcja kryptografii asymetrycznej
- Ochrona poufności i ochrona autentyczności w kryptografii asymetrycznej

Klucze sesyjne, dystrybucja kluczy sesyjnych

- Koncepcja klucza sesyjnego
- Problemy dystrybucji klucza sesyjnego
- Dystrybucja klucza sesyjnego z wykorzystaniem kryprografii asymetrycznej
- Procedura Diffiego-Helmanna

Infrastruktura klucza publicznego

- Problem wiarygodności kluczy publicznych
- Koncepcja Centrum Dystrybucji Kluczy
- Zadania CDK
- Certyfikaty kluczy publicznych
- Zastosowania praktyczne w komunikacji sieciowej

Funkcje jednokierunkowe – zastosowania w ochronie informacji

- Istota funkcji jednokierunkowej
- Implementacje praktyczne funkcji jednokierunkowych (MD5, SHA i inne)
- Zastosowania funkcji jednokierunkowych – hasła jednokrotne (procedura Lamporta), „hashowanie” haseł

Podpis cyfrowy

- Wykorzystanie kryptosystemów symetrycznych
- Wykorzystanie kryptosystemów asymetrycznych

Protokoły kryptograficzne w komunikacji sieciowej

- Protokół oparty na współdzieleniu klucza „każdy z każdym”
- Protokół szeroko-ustnej żaby
- Protokół z CDK generującym klucze
- Protokół oparty na kryptografii klucza publicznego
- Bardziej zaawansowane protokoły – przykład protokołu Kerberos
- Zasady tworzenia bezpiecznych protokołów kryptograficznych

Szyfry blokowe a szyfry strumieniowe

- Zasady działania szyfrów blokowych
- Tryby działania szyfrów blokowych
- Zasady działania szyfrów strumieniowych

Współczesne implementacje szyfrów

- IDEA
- DES, Modyfikacje algorytmu DES
- AES
- RSA
- Inne algorytmy z kluczem publicznym

Zastosowania kryptografii w systemach informatycznych

- Szyfrowanie plików i dysków
- Szyfrowanie połączeń internetowych (SSL, TSL, https)
- Wirtualne sieci prywatne (VPN)
- Szyfrowanie sesji terminalowych i poczty
- Szyfrowanie sprzętowe połączeń telekomunikacyjnych

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **RBP**

Tytuł: **Rekomendacja KNF dot. bezpieczeństwa płatności internetowych**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

Program

Na szkoleniu prezentowane jest 14 rekomendacji KNF, zawartych w dokumencie „Rekomendacja dot. bezpieczeństwa płatności internetowych". Każda z rekomendacji jest szczegółowo omawiana. Dyskutowane są sposoby wdrożenia poszeczególnych wymogów Nadzorcy oraz dokonywana jest ocena, czy dana rekomendacja jest już w Bankach wdrożona.

Omawiane są zatem następujące rekomendacje:

Rekomendacja 1: Polityka bezpieczeństwa

Rekomendacja 2: Ocena ryzyka

Rekomendacja 3: Monitorowanie i raportowanie incydentów

Rekomendacja 4: Kontrola i przeciwdziałanie ryzyku

Rekomendacja 5: Śledzenie (ang. traceability)

Rekomendacja 6: Wstępna identyfikacja klienta, informacje

Rekomendacja 7: Silne uwierzytelnianie klienta

Rekomendacja 8: Wnioskowanie o narzędzia uwierzytelniające i/lub oprogramowanie oraz ich dostarczanie

Rekomendacja 9: Próby logowania, wygasanie sesji, ważność uwierzytelnienia

Rekomendacja 10: Monitorowanie transakcji

Rekomendacja 11: Ochrona wrażliwych danych płatniczych

Rekomendacja 12: Edukacja i komunikacja z klientami

Rekomendacja 13: Powiadomienia, ustalanie limitów

Rekomendacja 14: Dostęp dla klientów do informacji o statusie inicjacji i wykonania płatności

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **WPCD**

Tytuł: **Warsztaty tworzenia Planów Ciągłości Działania**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

- Szkolenie ma charakter **warsztatowy**, co oznacza, że uczestnicy uczą się umiejętności budowania Planów Ciągłości Działania (PCD) w formie praktycznych ćwiczeń.
- Podstawą ćwiczeń są rzeczywiste procesy funkcjonujące w Bankach Spółdzielczych.

Program

Szkolenie rozpoczyna się od krótkiego wykładu, wprowadzającego podstawowe pojęcia (SZCD, PCD, procedury odtworzeniowe, procesy, MAK, RTO, RPO) po którym następuje forma ćwiczeniowa.

Każdy z uczestników wybiera sobie przykładowy proces biznesowy (np. z własnego Banku) i dla tego procesu tworzy:

- kartę procesu z określeniem ścieżki jego przebiegu oraz parametrów RTO i RPO,
- listę komórek organizacyjnych / stanowisk, w których realizowane są poszczególne etapy procesu,
- listę niezbędnych zasobów infrastrukturalnych, ludzkich, informatycznych i usług zewnętrznych, niezbędnych do zrealizowania procesu w środowisku alternatywnym (MAK),
- procedury odtworzeniowe zasobów (procedury awaryjne).

Po wykonaniu każdego z powyższych ćwiczeń, każdy z uczestników odczytuje wynik swojej pracy i jest on poddawany weryfikacji przez wykładowcę.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **TAB**

Tytuł: **Przeprowadzanie testów penetracyjnych w niewielkich sieciach heterogenicznych - warsztaty**

Liczba dni: **1**

Wykładowca: **dr inż. Tomasz Wasiak (Kerberos oraz Politechnika Łódzka)**

UWAGA: Szkolenie ma charakter laboratoryjny – Słuchacze pracują na **własnych, przywiezionych** ze soba laptopach!

Cel

Celem szkolenia jest wyposażenie Uczestników w praktyczną umiejętność przeprowadzania okresowych, technicznych audytów bezpieczeństwa własnej infrastruktury informatycznej, polegających na wykonywaniu skanowań i testów penetracyjnych serwerów, stacji roboczych oraz urządzeń sieciowych.

Program

1. Wprowadzenie do analizy sieci (adresacja tcp/ip i MAC)

2. Rozpoznanie struktury sieci i wpiętych w nią urządzeń

3. Analiza otwartych usług i wersji oprogramowania (narzędziami netcat, nmon, itp)

4. Wyszukiwanie podatności w wykrytych usługach (openvas)

5. Analiza rodzajów podatności i metod ich wykorzystania (w tym: Denial of service, przejęcie konta przy wykorzystaniu podatności, brute-force)

6. Symulacja ataków na środowisko za pomocą znalezionych podatności (metasploit)

7. Łatwe metody zabezpieczania przed atakiem

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kod: **ASL**

Tytuł: **Wprowadzenie do administrowania systemem Linux - warsztaty**

Liczba dni: **1**

Wykładowca: **dr inż. Tomasz Wasiak (Kerberos oraz Politechnika Łódzka)**

UWAGA: Szkolenie ma charakter laboratoryjny – Słuchacze pracują na **własnych, przywiezionych** ze soba laptopach!

Program

1. Podstawowe komendy w trybie konsolowym (praca z katalogami, plikami)
2. Rodzaje uprawnień w środowisku linux: "drwx", suid/guid, get/setfacl
3. Narzędzia administratora serwera linux:

    -najczęściej spotykany edytor -vi/vim może być łatwy w obsłudze

    -ułatwienia przy pracy w konsoli: np. screen

    -aplikacje pomagające w pracy na plikach/strumieniach: grep, awk, sed, sort, diff/vimdiff, find, du

4. Konfiguracja środowiska:

    -ln

-zmienne środowiskowe

    -aliasy

    -sudo

5. Analiza wydajności i obciążenia systemu (w tym symulacje przeciążania): cpu, RAM, dyski
6. Kontrola sieci: netcat, tcpdump itp.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZSW**

Tytuł: **Zabezpieczanie systemu Windows – warsztaty**

Liczba dni: **1**

Wykładowca: **dr inż. Tomasz Wasiak (Kerberos oraz Politechnika Łódzka)**

UWAGA: Szkolenie ma charakter laboratoryjny – Słuchacze pracują na **własnych, przywiezionych** ze soba laptopach!

Program

1. Podsumowanie mechanizmów zabezpieczeń w systemach Windows.

1.1 Uwierzytelnianie
1.1.1 Konta
1.1.2. Grupy
1.1.3 Polityka haseł i kont
1.1.4 Zarządzanie hasłami
1.1.5 Certyfikaty
1.1.6 Protokoły uwierzytelniania
1.1.7 Relacje zaufania

1.2 Autoryzacja
1.2.1 Zarządzanie usługą katalogową
1.2.2 "Shared Folders"
1.2.3 Uprawnienia NTFS
1.2.4 Uprawnienia drukowania
1.2.5 Uprawnienia rejestru

1.3 Inspekcja

1.4 Monitorowanie

1.5 Utwardzanie

1.6 Szyfrowanie

1.7 Standaryzacja

1.8 AntiSpyware, Antivirus

1.9 Filtrowanie pakietów

1.10 Aktualizowanie i skanowanie

2. GPO.

2.1 Wprowadzenie

2.2 Budowa GPO

2.3 Tworzenie i przechowywanie GPO

2.4 Przetwarzanie GPO

2.5 Filtrowanie zasięgu i delegowanie kontroli nad GPO

2.6 MMC dedykowane do pracy z GPO

2.7 Zalecenia jak tworzyć i wdrażąc GPO

3. Inspekcja i monitorowanie zabezpieczeń.

3.1 Inspekcja zdarzeń

3.2.1 Monitorowanie inspekcji
3.2.2 Inspekcja i jej monitorowanie - zalecenia
3.2.3 Narzędzia dodatkowe
3.2.4 Monitorowanie udziałów sieciowych
3.2.5 Monitorowanie sieci

4. Szyfrowanie EFS.

4.1 Wprowadzenie

4.2 Funkcje dodatkowe

4.3 Wady i zalety EFS

4.4 EFS na komputerach w grupie roboczej

4.5 EFS na komputerach w domenie z PKI

4.6 Kopiowanie plików wśrodowisku EFS

4.7 Przesyłanie zaszyfrowanych plików

4.8 Zalecenia konfiguracyjne

5. Dystrybucja "łatek".

5.1 Wprowadzenie

5.2 WSUS - Windows Server Update Services

5.3 WSUS - Konfiguracja klientów

5.4 WSUS - Przenoszenie bazy

5.5 WSUS - Raportowanie

6. Sprawdzanie stanu bezpieczeństwa.

6.1 MBSA

6.2 Wnterprise Update Scan Tool - EST

6.3 DumpSec

6.4 GFI LanGuard, Retina eEye Scanner, Nessus, Nmap

6.5 Skanowanie pod katem oprogramowania Spyware

6.6 Microsoft Windows Malicious Software Removal Tool

6.7 Produkty Microsoft - linia antispyware, antivirus

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZSL**

Tytuł: **Zabezpieczanie systemu Linux – warsztaty**

Liczba dni: **1**

Wykładowca: **dr inż. Tomasz Wasiak (Kerberos oraz Politechnika Łódzka)**

UWAGA: Szkolenie ma charakter laboratoryjny – Słuchacze pracują na **własnych, przywiezionych** ze soba laptopach!

Program

1. Uruchomienie i konfiguracja „bezpiecznego" systemu GNU Linux

   a. Zabezpieczenie jądra w oparciu o pakiet grsecurity

      i.Zabezpieczenie przed przepełnieniem stosu

      ii.Zabezpieczenie przed wykonaniem kodu w pamięci

      iii.Zabezpieczenie przed nieznanymi exploitami

   b. Bezpieczne zarządzanie serwerem

      i.Konfiguracja kont użytkowników

      ii.Autoryzacja użytkowników w oparciu o tradycyjne hasło

      iii.Autoryzacja użytkowników w oparciu o klucze niesymetryczne

   c. Przydzielanie limitów w dostępie do zasobów sprzętowych
   d. Bezpieczne podłączanie nośników pamięci

      i.Zabezpieczanie przed nieautoryzowanym wykonaniem kodu

      ii.Rozszerzona konfiguracja dostępu do plików w oparciu o ACL

   e. Konfiguracja filtrowania pakietów z uwzględnieniem stanów połączeń
   f. Delegowanie uprawnień dla użytkowników poprzez mechanizm sudo
   g. Zabezpieczenia usług sieciowych - tcpwrapper

2. Nadzorowanie istniejącego systemu Linux

   Konfiguracja mechanizmu logowania syslog
   Rotowanie logów dziennika systemowego i jego automatyczne składowanie
   Omówienie sposobów analizy dzienników systemowych – logwatch
   Graficzne narzędzia do analizy ruchu sieciowego – ntop, mrtg i inne
   Weryfikacja integralności systemu operacyjnego – rkhunter,tripwire i podobne
   Analiza dostępności i poziomu usług w systemach z rodziny GNU Linux
   Weryfikacja bezpieczeństwa systemu operacyjnego – Nessus

3. Zabezpieczanie popularnych usług sieciowych: samba, ftp

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZOI**

Tytuł: **Zarządzanie obszarem informatyki w Banku**

Liczba dni: **1**

Wykładowca: **Roland Węgrzynowski, Gospodarczy BS w Barlinku**

Podczas szkolenia omówione będą następujące zagadnienia:

- Podstawy budowania i zarządzania zespołu - wprowadzenie,
- Zadania zespołu IT – wyznaczanie zadań
- Utrzymanie niskiej fluktuacji zespołu IT
- Rozwój kompetencji zespołu IT

Program

Podstawy budowania i zarządzania zespołu - wprowadzenie,

Kompetencje

Podział zadań

Wprowadzanie zmian

Rozwiązywanie konfiktów

Elastyczne rozwiązywanie problemów

Zadania zespołu IT – wyznaczanie zadań

Podział podstawowych obowiązków wynikających z Rekomendacji D

Zadania „specjalne”

Co potrafi informatyk

Ile jest w stanie wykonać

Utrzymanie niskiej fluktuacji zespołu IT

Wyzwania
Motywatory pozafinansowe

Rozwój kompetencji zespołu IT
Kursy i szkolenia
Konferencje, wymiana doświadczeń

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **WPCD**

Tytuł: **Warsztaty tworzenia Planów Ciągłości Działania**

Liczba dni: **1**

Wykładowca: **dr inż. Albert Sadowski (Kerberos oraz WSH w Radomiu)**

- Szkolenie ma charakter **warsztatowy**, co oznacza, że uczestnicy uczą się umiejętności budowania Planów Ciągłości Działania (PCD) w formie praktycznych ćwiczeń.
- Podstawą ćwiczeń są rzeczywiste procesy funkcjonujące w Bankach Spółdzielczych.

Program

Szkolenie rozpoczyna się od krótkiego wykładu, wprowadzającego podstawowe pojęcia (SZCD, PCD, procedury odtworzeniowe, procesy, MAK, RTO, RPO) po którym następuje forma ćwiczeniowa.

Każdy z uczestników wybiera sobie przykładowy proces biznesowy (np. z własnego Banku) i dla tego procesu tworzy:

- kartę procesu z określeniem ścieżki jego przebiegu oraz parametrów RTO i RPO,
- listę komórek organizacyjnych / stanowisk, w których realizowane są poszczególne etapy procesu,
- listę niezbędnych zasobów infrastrukturalnych, ludzkich, informatycznych i usług zewnętrznych, niezbędnych do zrealizowania procesu w środowisku alternatywnym (MAK),
- procedury odtworzeniowe zasobów (procedury awaryjne).

Po wykonaniu każdego z powyższych ćwiczeń, każdy z uczestników odczytuje wynik swojej pracy i jest on poddawany weryfikacji przez wykładowcę.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **PSD**

Tytuł: **Wdrożenie dyrektywy PSD w systemach Bankowości Internetowej**

Liczba dni: **1**

Wykładowca: **Andrzej Dubis, Podkarpacki BS w Sanoku**

W związku z wejściem w życie Dyrektywy PSD II, przed organizacjami finansowymi pojawiły się nowe wyzwania. Jednym z nich jest konieczność przygotowania przez Bank API, z którego korzystać będą mieli możliwość zewnętrzni dostawcy łączący się z Systemami Bankowości Internetowej.

Podczas szkolenia omówione zostaną m.in. kwestie zw. z opisem interfejsów w zakresie PSD II, sposobów traktowania przez dyrektywę PSD II bezpieczeństwa danych oraz wymogów wykonania API, bezpieczeństwem płatności elektronicznych po umożliwieniu dostępu do rachunku osobom trzecim czy problematycznym tematem czy Dyrektywa naprawdę zwiększy konkurencyjność podmiotów finansowych. Przedstawiony zostanie aktualny status prac w zakresie PolishAPI oraz inne dostępne na rynku API możliwe do wykorzystania.

Program

I. Dostęp do rachunku bankowego podmiotów trzecich (TPP)

Na jakich zasadach. Podstawowe rodzaje usług AIS, PIS, COF. Rola Banku w realiach PSD2 – obowiązki i prawa.

II. Silne uwierzytelnienie klienta (SCA)

Co trzeba spełnić aby być zgodnym. Jakie operacje/czynności użytkownika trzeba silnie autoryzować a gdzie można zrobić wyjątki. Monitoring transakcji wykonywanych przez bankowość internetową. Kto odpowiada za nieautoryzowane transakcje.

III. Polish Api

Jak wygląda budowa otwartego standardu. Aktualny status prac. Co uwzględnione zostało w projekcie jako wymóg a co będzie usługami typu Premium. Rodzaje i obszary usług w API. Rola HUB-a w KIR z uwzględnieniem założeń biznesowych.

IV. Budowa własnego API z pomocą dostępnych narzędzi informatycznych

Czy warto stworzyć własne API. Dostępne na rynku oprogramowanie na przykładzie. Wady i zalety takiego rozwiązania.

V. Czy Banki zostaną tylko procesorem usług – jaką rolę uczestnika procesu wybrać ?

Omówienie czterech głównych możliwych scenariuszy. Wady i zalety poszczególnych rozwiązań. Którą opcje wybrać w zależności od możliwości finansowych i oczekiwań biznesu.

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnej organizacji.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Kod: **ZRIT**

Tytuł: **Zarządzanie Ryzykiem IT w Banku**

Liczba dni: **1**

Wykładowca: **Damian Nawrocki, BS w Jastrzębiu Zdroju**

Program

- Pojęcie ryzyka
- Koncepcje zarządzania ryzykiem
- Przegląd standardów związanych z zarządzaniem ryzykiem (ISO 31000:2009 i 31000:2012, COSO II, FERMA)
- Ryzyko systemów informatycznych
- Standardy związane z ryzykiem systemów
- informatycznych
- Podejście do analizy ryzyka systemów informatycznych
- Identyfikacja zagrożeń, podatności i środowiska
- Szacowanie ryzyka - przegląd metod
- Ograniczanie ryzyka
- Monitorowanie i reagowanie na zmiany
- Zarządzanie ryzykiem w procesie bezpieczeństwa informacji
- Zarządzanie ryzykiem w procesie ciągłości działania
- Zarządzanie ryzykiem w projekcie informatycznym
- Ryzyko w zarządzaniu strategicznym IT

Konsultacje i pytania do wykładowy

Po zakończeniu szkolenia, osoby zainteresowane będą mogły pozostać na **sesję konsultacji i pytań** do Wykładowcy. W trakcie tej sesji będzie można skorzystać z porad i praktycznych wskazówek, zadać pytania wykładowcy i przedyskutować rzeczywiste problemy, występujące we własnym Banku Spółdzielczym.

Sesja konsultacji i pytań przeznaczona jest dla osób chętnych.

Kerberos
OCHRONA INFORMACJI

Formularz zgłoszeniowy

Uprzejmie prosimy o wypełnienie na komputerze, nie odręcznie – dziękujemy!

Kod szkolenia lub tytuł	
Data	
Miejsce, godziny	Warszawa, Instytut Biocybernetyki PAN, u. Trojdena 4 Wykłady w godzinach: 10:00 – 15:00
Koszt udziału jednego uczestnika	490 zł + VAT (23%)
Liczba zgłaszanych osób	

UWAGA: Instytuty Biocybernetyki PAN dysponuje hotelem (w tym samy budynku, w którym odbędzie się szkolenie), tel. do hotelu: 22 668 50 17

Lp.	Imię i nazwisko oraz stanowisko uczestnika szkolenia	E-mail do uczestnika szkolenia	Telefon do uczestnika
1			
2			
3			
4			

Dane do faktury:	
Nazwa instytucji	
Dokładny adres	
Numer identyfikacyjny NIP	
Tel/fax	

Oświadczam, iż kwota _____ zł zostanie przekazana na konto Kerberos Sp. z o.o. po otrzymaniu faktury za szkolenie. Niniejsze zgłoszenie stanowi upoważnienie do wystawienia faktury VAT bez podpisu potwierdzającego jej odbiór.

Firma Kerberos Sp. z o. o. zastrzega sobie prawo do przesunięcia terminów na późniejsze (ustalone w porozumieniu z zarejestrowanymi uczestnikami). Rezygnacja z udziału w szkoleniu nie później niż na 7 dni przed terminem szkolenia oraz nieobecność na szkoleniu powoduje powstanie zobowiązania pokrycia pełnych kosztów udziału na podstawie faktury Kerberos Sp. z o. o..

(prosimy o odznaczenie - w przypadku wyrażenia zgody)
[ ]Wyrażam zgodę na przetwarzanie podanych powyżej danych w celu informowania o organizowanych seminariach, konferencjach, szkoleniach oraz usługach i produktach oferowanych przez firmę Kerberos Sp. z o. o zgodnie z ustawą o ochronie danych osobowych (Dz. U. Nr 133/97, poz. 883). Firma Kerberos Sp. z o. o. informuje o przysługującym Państwu prawie do wglądu i modyfikacji swoich danych osobowych.

_____ Data i podpis osoby uprawnionej do akceptacji kosztów

_____ Pieczęć instytucji