Program

15 godzin wykładowych

- Podstawy środowiska i procesów IT w międzynarodowej instytucji finansowej
- Technologie związane ze środowiskiem pracy użytkownika końcowego
- Zarządzanie ciągłością biznesową
- Platformy serwerowe i usługa katalogowa Active Directory
- Bazy danych w środowisku korporacyjnym
- Aplikacje Webowe – przegląd platform oraz wybranych aspektów zarządzania ryzykiem IT
- Zarządzanie zmianą oraz prowadzenie projektów informatycznych w środowisku wielokulturowym

15 godzin zajęć laboratotoryjnych

- Praktyczne wprowadzenie do procesów ITIL – symulacja obsługi incydentu (Major Incident)
- Przedstawienie współczesnych technik i typów wirtualizacji w obszarze rozwiazań desktopowych
- Zarządzanie ciągłością biznesową w praktyce
- Zbudowanie bezpiecznego mechanizmu single sign-on w oparciu o MS AD oraz Kerberos dla aplikacji web w środowisku Microsoft/Linux
- Zapoznanie się ze znaczeniem ról poszczególnych interesariuszy w projekcie bazy danych w środowisku korporacyjnym
- Zapoznanie się z narzędziami do wykrywania luk w aplikacjach web
- Rozumienie wymagań biznesowych i ich przełożenie na projekty IT

Informacje

Kurs jest adresowany do studentów kierunków Informatyka i Teleinformatyka

- II stopień, stacjonarna (1 i 3 semestr)
- I stopień semestr 6

Kod kursu: INEW00100

Język kursu: **polski**

Termin:

- wykład we wtorki od 17.00 do 18.30 (co 2 tygodnie)
- laboratorium (co 2 tygodnie naprzemiennie) – wtorek 15.00 lub 17.00

Zapisy w przerwie międzysemestralnej przez system JSOS oraz osobiście w trakcie pierwszego wykładu

- Liczba punktów ECTS: 3 (punkty będą zaliczane do suplementu dyplomu)
- **Osoby które ukończą kurs otrzymają imienne certyfikaty z Credit Suisse**
- Uwaga! Ze względu na specyfikę zajęć (2 grupy laboratoryjne) – liczba miejsc jest ograniczona do 36
- Wykład 1: Politechnika, 8 marca 2016, od 17.00 do 18.30

Zapraszamy wszystkich zaintersowanych studentów na Wykład Inauguracyjny:

Credit Suisse
Green Day, Szczytnikca 9
1 marca 2016, g.18.00

Konktat:
marta.mazurek@credit-suisse.com

Politechnika Wrocławska

CREDIT SUISSE

Dołącz do kursu

Nowoczesna infrastruktura i bezpieczeństwo IT w globalnej firmie

Interesujesz się nowoczesnymi trendami w IT?

Intrygują Cię „tajniki" działania IT w środowisku korporacyjnym?

Chesz dowiedzieć się więcej o ITIL?

Scenariusz

Tłem dla kursu jest **incydent hakerski** do którego doszło w wyimaginowanej **firmie X**. Zdarzenie to miało wpływ na działalność operacyjną i renomę instytucji. Dogłębna analiza wykonana po zdarzeniu pozwoliła na ustalenie chronologii zdarzeń...

0. Social
Grupa hakerów przygotowuje się do ataku na instytucję finansową. Obserwuje jej pracowników na LinkedIn i czeka na okazję do rozpoczęcia ataku. Jeden z dyrektorów firmy (Krzysztof B.), potwierdza publicznie swój udział konferencji, dla osób decydujących o strategii IT dużych firm. Po kilku dniach w niej uczestniczy.

1. Phishing
Krzysztof B. otrzymuje email z prośbą o ocenę konferencji. Zachęcony nagrodą odpowiada "Tak" na pytania, pojawiające się w wyskakujących okienkach. Link ze spreparowanego emaila prowadził do strony wykorzystującej podatności znanych przeglądarek. Krzysztof B. nieświadomie, pozwolił za zainstalowanie Malware, który teraz działa w kontekście jego użtkownika.

2. Software
Malware na laptopie Krzysztofa stale monitoruje procesy systemu operacyjnego w celu przechwycenia tokena z obszaru LSA. By dostać jak najwyższe uprawnienia uszkadza rejestry systemowe, tym samym powodując efekt braku komunikacji komputera z domeną. Wymusza to reakcje drugiej linii wsparcia z uprawnieniami administratora domeny.

3. Network
Po przechwyceniu uprawnień administratora domeny, Malware uruchamia szyfrowany kanał na zewnątrz firmy pozwalający zdalnie wykonywać skrypty PowerShell wewnątrz infrastruktury firmy.

4. Data
Wykorzystując brak segregacji uprawnień i zdobyte mocne uprawnienia, atakujący dostają się do baz danych z których kradną dana osobowe klientów oraz dane ich kart kredytowych.

5. Incident
Atakujący w ramach zacierania śladów, czyszczą logi atakowanych serwerów oraz rozpoczynają atak DoS na podstawową infrastrukturę firmy. Przestają działać serwisy internetowe, komputery pracowników w punktach obsługi oraz większość serwerów i laptopów wewnątrz siedziby firmy.

6. Finance
Atakujący za pomocą siatki "słupów" na całym świecie, wypłaca możliwie jak najwięcej środków z przechwyconych kart kredytowych.

7. Reputation
Opinia publiczna dowiaduje się o problemach z działaniem serwisów i punktów obsługi instytucji finansowej. Infolinia pod naporem połączeń przestaje działać.

8. Defense
Powołany zostaje sztab zarządzania kryzysowego, któremu po długiej walce udaje się opanować sytuację.

9. Future
Po zażegnaniu kryzysu powołany do życia zostaje projekt / grupa projektów (top iniative) sponsorowany przez zarząd firmy, który ma za zadanie zapobiec podobnym sytuacjom w przyszłości.