

Cyberbezpieczeństwo

Mechanizmy obrony przed atakami hakerskimi

Cele szkolenia

Celem szkolenia jest przekazanie uczestnikom wiedzy na temat tworzenia skutecznych, kompleksowych zabezpieczeń przed wszelkimi zagrożeniami od strony hakerów. Uczestnik w trakcie szkolenia nauczy się rozpoznawać metody i techniki wykorzystywane przez hakerów oraz jak się przed nimi bronić.

Podczas szkolenia, uczestnik dowie się:

- Jak stworzyć kopie zapasowe minimalizujące skutki awarii?
- Jak skonfigurować bezpieczne środowisko?
- Jak poprawnie zarządzać ryzykiem w kontekście cyberbezpieczeństwa?
- Jak poprawnie zarządzać zagrożeniami, podatnościami i incydentami?
- O co zadbać podczas tworzenia aplikacji webowej?
- O konsekwencjach prawnych incydentów
- O wymogach prawnych dotyczących cyberbezpieczeństwa
- O dobrych praktykach i standardach wspierających bezpieczeństwo
- Narzędziach pomagających w osiągnięciu wysokiego poziomu bezpieczeństwa

Dzięki omówieniu powyższych zagadnień w oparciu o realne przypadki ataków i metod obrony przed nimi uczestnik poszerzy swoją wiedzę z zakresu cyberbezpieczeństwa o metody rozpoznawania, analizy i reagowania na zagrożenia jakie mogą spotkać każdego w dzisiejszych realiach branży IT. Zbuduje także solidne podstawy pod dalszy rozwój w obszarze cybersecurity.

Umiejętności

Dzięki szkoleniu uczestnik będzie:

- Identyfikował zagrożenia cyberbezpieczeństwa
- Przeprowadzał analizę słabych punktów swojego systemu
- Wiedział, jak poprawić bezpieczeństwo swojego systemu oraz aplikacji
- Tworzył bezpieczny, zgodny z dobrymi praktykami backup dla swojej organizacji
- W bezpieczny sposób zarządzał dostępem użytkowników
- Znał różnicę między antywirusem a EDR

- Prawidłowo reagował w przypadku incydentu bezpieczeństwa
- Znał regulacje odnoszące się do bezpieczeństwa danych.

Profil uczestników

Szkolenie skierowane jest do każdego użytkownika administratora, wdrożeniowca, DevOpsa i programisty który chce podnieść bezpieczeństwo efektów swojej pracy oraz całej organizacji, w szczególności dla osób pracujących na co dzień z danymi poufnymi.

Kurs jest skierowany m.in. do:

- początkujących jak i weteranów branży IT
- właścicieli i administratorów stron internetowych
- osób zarządzających sieciami teleinformatycznymi i serwerami
- osób prywatnych chcących poszerzyć swoją wiedzę z zakresu cyberbezpieczeństwa

Szkolenie jest skierowane do osób zarówno początkujących jak i posiadających podstawową wiedzę z zakresu cyberbezpieczeństwa którą dzięki szkoleniu będą mogli poszerzyć i uporządkować.

Dzięki poznaniu podstaw cybersecurity każda osoba będzie mogła lepiej zadbać o bezpieczeństwo swoje, bliskich a także swoich działalności co pozwoli na minimalizację ryzyka związanego z atakami hakerskimi. Umiejętności zdobyte podczas szkolenia pozwolą znacząco zmniejszyć zagrożenia związane z utratą pieniędzy, wrażliwych danych bądź pogorszeniem wizerunku.

Przygotowanie uczestników

Od uczestników wymagana jest znajomość podstawowych pojęć związanych z sieciami komputerowymi, systemami operacyjnymi oraz aplikacjami webowymi.

Szczegółowy program szkolenia

1. Przypomnienie podstawowych pojęć
2. Bezpieczeństwo sieciowe
 - 2.1. Bezpieczna architektura
 - 2.2. Bezpieczeństwo portów
 - 2.3. Zapory sieciowe
 - 2.4. Systemy IPS, IDS
 - 2.5. Logowanie ruchu
3. Bezpieczeństwo środowiska

- 3.1. Antywirus
- 3.2. Przechowywanie sekretów
- 3.3. Izolacja i wirtualizacja
- 3.4. Bezpieczna konfiguracja
- 3.5. Hardening
4. Bezpieczeństwo aplikacji
 - 4.1. Bezpieczne aplikacje webowe
 - 4.2. Kontrola dostępu
 - 4.3. Parsowanie danych
 - 4.4. Biblioteki dynamiczne i inne zależności
 - 4.5. Obfuskacja
 - 4.6. SAST
 - 4.7. DAST
 - 4.8. ASVS
5. Łańcuch dostaw
 - 5.1. Czym jest i jak wykorzystują go hakerzy
 - 5.2. Jak się przed tym bronić
6. Zarządzanie dostępem
 - 6.1. Modele kontroli dostępu
 - 6.2. IAM/SSO
 - 6.3. Moduły PAM
7. Zarządzanie incydentami bezpieczeństwa
 - 7.1. Przygotowania do incydentu
 - 7.2. Wykrywanie
 - 7.3. Analiza
 - 7.4. Reakcja
 - 7.5. Wyciąganie wniosków
8. EDR vs Antywirus
9. Spear Phishing
10. Bezpieczeństwo operacyjne
 - 10.1. Zarządzanie podatnościami
 - 10.2. Zarządzanie ryzykiem
 - 10.3. Planowanie zadań security, a biznes
 - 10.4. Regulamin RODO
 - 10.5. Procedury bezpieczeństwa
 - 10.6. SIEM/SOC
11. Live hacking – ataki na aplikacje webowe

Metoda realizacji szkolenia

Szkolenie będzie realizowane w formie:

- części teoretycznej w postaci prezentacji,
- kilku praktycznych i intuicyjnych ćwiczeń
- krótkiej części demonstracyjnej - live hacking

Forma szkolenia ma na celu przedstawienie w sposób atrakcyjny i interesujący wiedzy i technik związanych ze zwiększeniem poziomu cyberbezpieczeństwa w życiu prywatnym i zawodowym.

Kilka praktycznych demonstracji ataków - będzie polegało m.in. na rozpoznaniu rodzaju ataku, znalezieniu najlepszego sposobu zabezpieczenia swojej aplikacji/środowiska.

Liczba dni, liczba godzin szkoleniowych

2 dni, 16 godzin szkoleniowych

Ścieżka rozwoju po szkoleniu

Po zakończeniu szkolenia możliwe będzie kontynuowanie rozwoju w obszarach testów penetracyjnych, ochrony webaplikacji, bezpieczeństwa sieci, audytów bezpieczeństwa.