

Ankieta wstępna do audytu bezpieczeństwa infrastruktury sieciowej

Ankieta ma na celu zebranie podstawowych informacji o środowisku sieciowym do analizy, określenia potrzeb Klienta i przygotowania wyceny usługi.

Pytania ogólne

- 1 Ilość wszystkich hostów we wszystkich podsieciach:
 - a) Ilość laptopów/komputerów stacjonarnych: 100
 - b) Ilość serwerów (fizycznych i wirtualnych): 10
 - c) Ilość drukarek/skanerów sieciowych: 15
 - d) Ilość urządzeń brzegowych/Access Point/zarządzanych switchy: 20
 - e) Ilość kamer internetowych/rejestratorów: 17/2
- 2 Ilość odseparowanych podsieci: 14
- 3 Ilość użytkowników: 100

Dane teleadresowe

- 1 Imię i nazwisko osoby kontaktowej: Jarosław Serek
- 2 Adres email: jaroslaw.serek@wfos.krakow.pl
- 3 Numer telefonu: 785855625
- 4 Ilość audytowanych placówek: 1
- 5 Nazwa i adres audytowanych placówek: WFOSiGW w Krakowie, ul. Kanonicza 12, 31-002 Kraków
W przypadku więcej niż 1 placówki prosimy o podanie poniższych szczegółów dla każdej z nich osobno

1. Weryfikacja konfiguracji urządzenia brzegowego TAK/NIE

- 1.1. Ilość urządzeń: 6
- 1.2. Producent urządzenia: do przekazania po podpisaniu umowy
- 1.3. Model: do przekazania po podpisaniu umowy

2. Testy zdalne adresów publicznych TAK/NIE

- 2.1. Ilość adresów publicznych

3. Sieć WiFi TAK/NIE

- 3.1. Ilość sieci: 3

4. Weryfikacja aplikacji webowych TAK/NIE

- 4.1. Ilość aplikacji: 1

5. Socjotechnika

~~TAK~~/NIE

5.1. Kampania phishing

TAK/NIE

5.2. Kontakt bezpośredni

TAK/NIE

5.3. Kontakt telefoniczny

TAK/NIE

6. Ankiety dla pracowników

TAK/~~NIE~~

ankiety sprawdzające wiedzę pracowników w zakresie zasad cyberbezpieczeństwa

Ankieta wstępna do audytu RODO

Ankieta ma na celu zebranie podstawowych informacji, określenie potrzeb Klienta i przygotowania wyceny usługi.

Dane administratora (może być pieczętka)

Wojewódzki Fundusz ochrony Środowiska i Gospodarki Wodnej w Krakowie, ul. Kanonicza 12,
31-002 Kraków

Ankieta RODO

1. Dominujący przedmiot działalności organizacji / firmy

Informację na ten temat dostępne tutaj:
<https://www.wfos.krakow.pl/o-funduszu/organizacja/>

2. Liczba wszystkich pracowników (współpracowników) oraz orientacyjną liczbę osób przetwarzających dane osobowe w organizacji (nie tylko pracownicy administracyjni)

Okolo 100 osób

3. Występujące działy w organizacji / firmie (np. księgowy, logistyczny, prawny), jeżeli takowe są

Tutaj schemat organizacyjny:
<https://www.wfos.krakow.pl/wp-content/uploads/2020/05/schemat-organizacyjny-2020.pdf>

4. Czy dane osobowe przechowywane przetwarzane są w jednym miejscu (pod jednym adresem) czy takich miejsc (adresów / oddziałów) jest kilka – proszę podać liczbę takich adresów

6 miejsc

5. W ramach jakich działań pozyskiwane są dane osobowe – za pośrednictwem telefonu, strony internetowej, poczty elektronicznej, tradycyjnej, w trakcie wizyty klienta w firmie

Wszystkie wymienione

6. Czy firma pełni rolę podmiotu przetwarzającego, czyli czy pracują Państwo na danych osobowych uzyskanych od innego Administratora, któremu świadczą Państwo usługi przetwarzając dane osobowe

tak

ds

7. Czy organizacja przekazuje lub przetwarza dane osobowe poza Europejskim Obszarem Gospodarczym – poza Unią Europejską? Jeśli tak, w jakich celach

nie

8. Czy są zawarte bądź negocjowane umowy, których przedmiotem jest powierzenie danych podmiotom trzecim (współpraca np. z biurem rachunkowym, szkoleniowcem BHP)

tak

9. Czy pracownicy są zapoznani z ogólnymi zasadami i przepisami dotyczącymi bezpieczeństwa danych osobowych przed rozpoczęciem czynności związanych z przetwarzaniem danych osobowych (szkolenia)

tak

10. Czy w firmie jest system (np. CRM, ERP) do obsługi procesów (ile systemów informatycznych posiada firma do przetwarzania danych osobowych)

5 systemów

11. Czy organizacja w jakimkolwiek względzie dostosowana jest do wytycznych RODO poprzez wdrożenia polityk, procedur, informacji, zgód

tak

12. Czy firma korzysta z usług chmurowych, jeśli tak to z jakich (czy dane osobowe są przechowywane w przestrzeni internetowej)

Aplikacje Google G Suite – dane osobowe mogą być przechowywane

Ankieta wstępna do audytu bezpieczeństwa aplikacji webowej / API

Ankieta ma na celu zebranie podstawowych informacji o aplikacji webowej /API do analizy, określenia potrzeb Klienta i przygotowania wyceny usługi.

1. Liczba ról w aplikacji

Użytkownik, merytorysta w funduszu, administrator

2. Liczba i krótki opis funkcjonalności / endpointów API

Funkcjonalność systemu przedstawia udostępniona instrukcja:
<https://docs.google.com/document/d/1Dcl0fl6Zjewv7vxdmoB6U5SdumwnATbqa81RkZclQ/edit>

3. Czy aplikacja jest dostępna publicznie z możliwością zarejestrowania się/zalogowania (wersja demo) – jeżeli tak, to prosba o dostarczenie adresu URL i dostępów?

Podczas testów możliwe jest stworzenie konta tymczasowego, ale wyłącznie na wersji produkcyjnej

4. Czy konta użytkowników w aplikacji zostaną dostarczone testerom?

Samodzielna rejestracja

5. Czy testerzy otrzymają dokumentację do aplikacji / API?

nie

6. Czy testerzy otrzymają kod źródłowy aplikacji?

nie

7. Czy należy wykluczyć pewne typy testów?

Zgodnie z zapytaniem testy mają być przeprowadzone metodą OWASP top 10 dla aplikacji webowych

8. Czy testy mogą zostać przeprowadzone zdalnie?

tak

9. Czy testy mają być przeprowadzone w określonych oknach czasowych?

Termin do ustalenia po podpisaniu umowy. Wstępnie testy powinny być prowadzone w godzinach popołudniowych gdy portal jest mniej dociążony użytkownikami.

10. Czy infrastruktura jest chroniona przez systemy WAF/IDS/IPS/Cloudflare?

Do ustalenia po podpisaniu umowy

11. Czy system WAF/IDS/IPS/Cloudflare będą aktywne w trakcie testów?

Do ustalenia po podpisaniu umowy

12. W jakiej technologii została stworzona aplikacja?

php

13. Jakiego typu jest testowane środowisko?

produkcja