|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa** | **Wymagane minimalne elementy usługi** |
|  | Zadanie | Usługa audytu bezpieczeństwa IT |
|  | Główne obszary audytu | Wykonanie audyt dokumentacji i procesów w zakresie  1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI)  / Krajowym Systemie Cyberbezpieczeństwa (KSC)  • wyznaczenie osoby do kontaktu – Art. 21 KSC  • przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC  • zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC  • zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC  • zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC  • zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC  • opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI  • monitorowanie i przegląd SZBI – Par. 20 KRI  • doskonalenie SZBI – Par. 20 KRI  • aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI  • inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI  • przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI  • postępowanie z ryzykiem – Par. 20 pkt 3) KRI  • zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI  • szkolenia i uświadamianie – Par. 20 pkt 6) KRI  • monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI  • monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI  • zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI  • ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI  • zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI  • zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI  • zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI  • zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI  • ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków  przetwarzania – Par. 20 pkt 11) KRI  • aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI  • minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI  • ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI  • stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI  • zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI  • zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI  • kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI  • zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI  2. Ocena wybranych aspektów bezpieczeństwa systemów  Informatycznych  • dokumentacja potwierdzająca wykonane działania wskazanego w ustawie  • opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne  • dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne  • dokumentacja procesu zarządzania incydentami  • aspekty techniczne do weryfikacji  3. Ocena dojrzałości wybranych procesów bezpieczeństwa  • ochrona przed kodem szkodliwym  • ochrona sieci i połączeń  • ochrona urządzeń końcowych  • zarządzanie tożsamością i autoryzacją dostępu  • ochrona fizyczna systemów IT  • bezpieczeństwo urządzeń drukujących  • zarządzanie podatnościami  4. Opracowanie raportu z audytu oraz uzupełnienie arkusza do Oceny  • Weryfikacja dokumentacji sieci, topologii sieci, kluczowych  elementów sieci  • Skanowanie sieci – rekonesans sieci: Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy  operacyjne działają na wykrytych hostach. W szczególności:  • skanowanie sieci w poszukiwaniu wszystkich podłączonych hostów  • wykrycie czy jest dostęp do innych podsieci z danej podsieci  • wykrycie usług działających na hostach podłączonych do sieci  • wykrycie podatności na wybranych hostach w sieci    5. Testy penetracyjne infrastruktury sieciowej, w tym w szczególności: skanowanie najistotniejszych hostów w sieci które zostały wybrane na podstawie wcześniejszej analizy, w tym: weryfikacja występowania luk bezpieczeństwa dla konkretnych usług, w zależności od wykrytej usługi weryfikacja haseł, weryfikacja dostępu użytkowników do odpowiednich usług, weryfikacja możliwości dostępu do usługi, weryfikacja luk bezpieczeństwa w systemie operacyjnym, weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich, weryfikacja haseł w usługach umożliwiających logowanie, sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł, weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych, weryfikacja zabezpieczeń urządzeń sieciowych  6. Zdalne testy adresów publicznych    7. Badanie ankietowe. Badanie ankietowe pracowników działu IT oraz pracowników Zamawiającego z wiedzy o bezpieczeństwie sieci i  procedurach IT stosowanych przez Zamawiającego. Grupa ankietowanych pracowników zostanie ustalona podczas Audytu.    8. Testy socjotechniczne, w tym:  • kontakt telefoniczny – do 10 osób  • kampanie phishingowe – możliwa dla całej organizacji  9. Wykonanie raportu zawierającego  • opis wszystkich elementów, które zostały poddane audytowi  • podział podatności ze względu na ryzyko: wysokie, średnie, niskie  • wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności  • wylistowanie wszystkich podatności ze względu na ryzyko: wysokie, średnie, niskie  • określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności  10. Wsparcie po audytowe |
|  | Uwaga | Audytor powinien posiadać uprawnienia zgodnie z obowiązującym prawem |