Znak sprawy BGP.271.9.2022

Załącznik nr 1

Audyt dokumentacji i procesów

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

1) wyznaczenie osoby do kontaktu – Art. 21 KSC
2) przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC
3) zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC
4) zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC
5) zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC
6) zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC
7) opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI
8) monitorowanie i przegląd SZBI – Par. 20 KRI
9) doskonalenie SZBI – Par. 20 KRI
10) aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI
11) inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI
12) przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI
13) postępowanie z ryzykiem – Par. 20 pkt 3) KRI
14) zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI
15) szkolenia i uświadamianie – Par. 20 pkt 6) KRI
16) monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI
17) monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI
18) zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI
19) ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI
20) zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI
21) zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI
22) zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI
23) zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI
24) ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – Par. 20 pkt 11) KRI
25) aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI

26) minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI
27) ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI
28) stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI
29) zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI
30) zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI
31) kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI
32) zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI

2. Ocena wybranych aspektów bezpieczeństwa systemów informatycznych

1) dokumentacja potwierdzająca wykonane działania wskazanego w ustawie
2) opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne
3) dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne
4) dokumentacja procesu zarządzania incydentami
5) aspekty techniczne do weryfikacji

3. Ocena dojrzałości wybranych procesów bezpieczeństwa

1) ochrona przed kodem szkodliwym
2) ochrona sieci i połączeń
3) ochrona urządzeń końcowych
4) zarządzanie tożsamością i autoryzacją dostępu
5) ochrona fizyczna systemów IT
6) bezpieczeństwo urządzeń drukujących
7) zarządzanie podatnościami

4. Opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny.

5. Opracowanie brakujących dokumentów zgodnych z SZBI.

6. Opracowanie i przekazanie Zamawiającemu załącznika nr 8 do projektu „Cyfrowa Gmina" w nieprzekraczającym terminie do dnia 18 sierpnia 2022 r. zgodnie z wytycznymi regulaminu Projektu „Cyfrowa Gmina"

- audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wykaz certyfikatów wskazanych w w/w rozporządzeniu znajduje się poniżej:

1. Certified Internal Auditor (CIA)
2. Certified Information System Auditor (CISA)
3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób
4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób
5. Certified Information Security Manager (CISM)
6. Certified in Risk and Information Systems Control (CRISC)
7. Certified in the Governance of Enterprise IT (CGEIT)
8. Certified Information Systems Security Professional (CISSP)
9. Systems Security Certified Practitioner (SSCP)
10. Certified Reliability Professional
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

Testy penetracyjne infrastruktury sieciowej

1. Przedstawienie założeń Audytu

Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy
i doświadczeń. Testy zostaną przeprowadzone w oparciu o OSSTMM (Open Source Security Testing Methodology Manual).

2. Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci

3. 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 ten etap polega na:

- skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów
- wykryciu czy jest dostęp do innych podsieci z danej podsieci
- wykryciu usług działających na hostach podłączonych do sieci
- wykryciu podatności na wybranych hostach w sieci

4. Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci

Przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania.

5. Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy

- 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

6. Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy

- weryfikacja haseł w usługach umożliwiających logowanie

7. Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł

8. Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych

9. Weryfikacja zabezpieczeń urządzeń sieciowych

- badanie odporności switchy na ataki sieciowe
- weryfikacja zabezpieczeń monitoringu wizyjnego

10. Zdalne testy adresów publicznych.

12. Wykonanie raportu zawierającego

- opis wszystkich elementów, które zostały poddane audytowi
- podział podatności ze względu na ryzyko:
  - wysoki
  - średni
  - niski
- wskazanie zaleceń, rekomendacji, najlepszych praktyk – dla każdej znalezionej podatności
- wylistowanie wszystkich podatności ze względu na ryzyko:
  - wysoki
  - średni
  - niski

- określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności

13. Wsparcie poaudytowe

Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.