OCENA WYBRANYCH ASPEKTÓW BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Zasady oceny

Każdemu z zagadnień, w polu oznaczonym na żółto, należy przypisać ocenę wg poniższej skali:

0	Całkowity brak realizacji wymagania. Brak świadomości wymogu.
1	Wymaganie spełnione w małym stopniu. Świadomość istnienia wymagania.
2	Częściowa realizacja wymagania.
3	Drobne niedociągnięcia, niewpływające na bezpieczeństwo IT.
4	Pełna zgodność z wymaganiami.

Lp.	Zagadnienie	Ustalenia	Ocena
1	**Dokumentacja potwierdzająca wykonane działania wskazanego w ustawie o krajowym systemie cyberbezpieczeństwa***		0
1.1	Czy zostały zidentyfikowane usługi publiczne, których świadczenie zależy od bezpieczeństwa systemów informacyjnych?		
1.2	Czy zostały wskazane osoby (podmioty) odpowiedzialne za zarządzanie incydentami?		
1.3	Czy podmiot publiczny realizuje zadania publikowania informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz możliwych, skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, tj. zadań zawartych w art. 22 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?		

1.4	Czy została wyznaczona i zgłoszona do właściwego CSIRT, osoba kontaktowa, o której mowa w art. 21 oraz art. 22 ust. 1 pkt 5 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.)?		
2	**Opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne**		0
2.1	Czy wszystkie elementy składowe systemu informatycznego zostały zinwentaryzowane?		
2.2	Czy dla każdego systemu informatycznego utrzymywana jest aktualna lista osób odpowiedzialnych za jego bezpieczną eksploatację?		
3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**		0
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?		
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?		
3.3	Czy istnieje dokumentacja architektury sieci?		
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?		
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?		
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?		

3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?		
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?		
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?		
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?		
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?		
4	**Dokumentacja procesu zarządzania incydentami**		0
4.1	Czy wdrożone jest monitorowanie i wykrywanie incydentów? Kto za nie odpowiada? (stanowiska, funkcje itp. - bez danych osobowych)		
4.2	Czy istnieje procedura informowania o wykrytych incydentach?		
4.3	Czy istnieją procedury reagowania na incydenty?		
5	**Aspekty techniczne do weryfikacji**		

5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.		0
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.		0
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.		0
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.		0

6	**Aspekty organizacyjne do weryfikacji**		
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.		0
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.		0

*Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.).