trecom

Mind Mapa obowiązków i odpowiedzialności **NIS 2 i UoKSC.**

Infografika autorstwa

Tomasza Matuły

NIS 2
BAZA WIEDZY

Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa

MAPA OBOWIĄZKÓW I ODPOWIEDZIALNOŚCI

Obowiązek samo rejestracji [Art. 7]

- Zgłoszenia dokonuje Kierownik Podmiotu
- Poprzez złożenie wniosku w systemie S46 [Art. 46]
- W terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny
- Wpis z urzędu dokonywany tylko dla
  - Przedsiębiorcy telekomunikacyjni
  - Dotychczasowi Operatorzy Usług Kluczowych
  - Dostawcy usług zaufania
  - Podmioty publiczne

Wyznaczenie osób odpowiedzialnych zautrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa [Art. 9]

- Podmiot kluczowy i ważny
  - Wyznacza co najmniej dwie osoby
- Podmiot kluczowy i ważny będący mikro- lub małym przedsiębiorcą
  - Wyznacza co najmniej jedną osobę

Opracowanie, stosowanie i aktualizacja dokumentacji dot. bezpieczeństwa systemu informacyjnego [Art. 10]

- Dokumentacja normatywna
- Dokumentacja operacyjna

Powołanie wewnętrznej struktury odpowiedzialnej za cybersec lub zawarcie umowy z dostawcą usług zarządzania w zakresie cybersec [Art. 14].

Przeprowadzanie audytu bezpieczeństwa systemu informacyjnego [Art. 15].

- Tylko podmioty kluczowe.
- Pierwszy audyt w ciągu 24 miesięcy.
- Kolejne audyty raz na trzy lata.
- Organ właściwy ds. cyberbezpieczeństwa może zawsze nakazać przeprowadzenie audytu ad hoc w drodze decyzji.

Informowanie o cyberzagrożeniu, incydencie użytkowników usług [Art. 11, ust. 2a i 2b].

- Na których poważne cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć.
- O samym poważnym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.
- O incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.

Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałanie przy obsłudze incydentu poważnego [Art. 11, 12, 13].

- Zapewnienie obsługi incydentów.
- Zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT.
- Klasyfikacja incydentów poważnych.
- **Zgłoszenie wczesnego ostrzeżenia o incydencie poważnym.**
  - Do CSIRT sektorowy.
  - Nie później niż w ciągu 24 godz. od wykrycia.
- **Zgłoszenie incydentu poważnego.**
  - Do CSIRT sektorowy.
  - Nie później niż w ciągu 72 godz. od wykrycia.
- Przekazanie sprawozdania okresowego.
  - Tylko gdy wnioskuje o to właściwy CSIRT sektorowy.
- **Przekazanie sprawozdania końcowego z obsługi incydentu poważnego.**
  - Do CSIRT sektorowy.
  - Nie później niż **w ciągu 1 miesiąca** od wykrycia.
- Współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT.
- Usuwanie podatności, o których mowa w art. 32 ust. 2 oraz informowanie o nich.
  - CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego.

(SZBI) Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w systemie informacyjnym [Art. 8].

- Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.
- Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych.
  - Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne.
  - Bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym **testowanie systemu informacyjnego.**
  - Bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu.
  - Bezpieczeństwo zasobów ludzkich.
  - Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT.
  - Wdrażanie, dokumentowanie, testowanie i utrzymywanie **planów ciągłości działania... planów awaryjnych, oraz planów odtworzenia działalności.**
  - Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi **systemem monitorowania w trybie ciągłym.**
  - Polityki i procedury oceny skuteczności środków technicznych i organizacyjnych.
  - Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu.
  - Podstawowe zasady cyber higieny.
  - Polityki i procedury stosowania kryptografii i szyfrowania (w stosownych przypadkach).
  - Stosowanie bezpiecznych środków komunikacji... (w s.p.) uwzględniających uwierzytelnianie wieloskładnikowe.
  - Zarządzanie aktywami.
  - Polityki kontroli dostępu.
  - Wdrożenie w terminie 12 mcy.
- Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego.
- **Zarządzanie incydentami.**
- Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego.
  - Stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.
  - Regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji.
  - Ochrona przed nieuprawnioną modyfikacją w systemie informacyjnym.
  - Niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego... mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności... usług.
- UWAGA: Podmioty publiczne-ważne.
  - Nie są objęte obowiązkiem wdrożenia pełnego SZBI.
  - Zamiast tego zobowiązane są do wdrożenia uproszczonego SZBI zgodnego z wymogami określonymi w załączniku nr 4 do ustawy,

KIEROWNIK PODMIOTU obowiązki i odpowiedzialności [Art. 8 c, d, e].

- Ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot.
  - UWAGA: Brak możliwości delegacji odpowiedzialności na CIO, CTIO, CISO itp.
- Podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI.
- Planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa.
- Przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie.
- Zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie.
- Zapewnia zgodność działania podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.
- Obligatoryjnie raz w roku lub częściej odbywa szkolenie w zakresie wykonywania obowiązków.

trecom | Cisco Partner

Potrzebujesz pomocy w obszarze NIS 2 lub UoKSC?

Umów się na bezpłatną konsultację i otrzymaj konkretne rekomendacje.

Jan Bręczewski

jan.breczewski@trecom.pl

+48 727 990 111

O Trecom

Jako Trecom od ponad 25 lat rozwijamy, optymalizujemy i utrzymujemy złożone systemy IT. Jesteśmy jednym z liderów rynku polskiego w segmencie sieci, cyberbezpieczeństwa, systemów AV, UC oraz data center. Nasz zespół składa się z ponad 115 inżynierów i architektów.

Posiadamy ponad 70 partnerstw technologicznych z wiodącymi dostawcami technologii oraz obszerną ofertę szkoleń. Rozbudowane portfolio rozwiązań przekłada się na niemal nieograniczone możliwości projektowe.

Nasza oferta obejmuje audyt, doradztwo, projektowanie, wdrażanie oraz utrzymywanie infrastruktury IT oraz cyberbezpieczeństwa. Wspieramy naszych klientów również poprzez usługi zarządzane – SOC, NOC i Centrum Wsparcia.