FZSZ 8.2 – Załącznik nr 2 do ZSZ8
Katalog incydentów i zdarzeń bezpieczeństwa informacji

1. Definicje:

- Zdarzenie związane z bezpieczeństwem informacji - zwane też zdarzeniem bezpieczeństwa – jest to określony stan systemu, usługi lub sieci, który wskazuje na niezgodność, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem (może wpływać na bezpieczeństwo) i może być przyczyną incydentu lub słabością systemu
- Słabość systemu lub zabezpieczenia, aktywu – stan, sytuacja lub właściwość która, może spowodować wystąpienia incydentu lub zdarzenia związanego z bezpieczeństwem informacji.
- Incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, stwarzających znaczne prawdopodobieństwo zakłócenia lub zatrzymania działań biznesowych i zagrażających bezpieczeństwu informacji zwłaszcza w odniesieniu do poufności , integralności i dostępności.

2. Pracownicy szpitala - zgłaszają Przewodniczącemu Zespołu ds. Bezpieczeństwem Informacji (obecnie PZJ) wszelkich zdarzeń i słabości związanych z naruszeniem zasad bezpieczeństwa informacji oraz poinformowanie o tym fakcie swojego przełożonego

3. Podział zdarzeń:

Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:

- nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony transfer danych,
- pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

4. Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2. Włamanie do obiektów Szpitala lub próba włamania
3. Sabotaż lub próba sabotażu
4. Utrata danych w systemach informatycznych

5. Utrata lub bezprawne zniszczenie dokumentów
6. Bezprawne wynoszenie aktywów poza siedzibę Szpitala
7. Pozostawienie osoby bez stosownych uprawnień w obszarze przetwarzania bez uprzedniego zabezpieczenia aktywów
8. Awarie krytycznej infrastruktury przetwarzania informacji (np. serwery, rutery, zasilania, itp.)
9. Zgubienie aktywów informacyjnych (np. dokumentów, telefon, laptop, klucze, pendrive, itp.)
10. Kradzież aktywów (np. dokumentów, telefon, laptop, klucze, pendrive, itp.)
11. Awarie budowlane zagrażające aktywom informacyjnym
12. Brak dostępu do aktywów dla osób uprawnionych
13. Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
14. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
15. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
16. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
17. Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
18. Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
19. Nastąpiła niedopuszczalna manipulacja danymi w systemie.
20. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
21. Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
22. Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
23. Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
24. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
25. Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).