Proces Zarządzania Podatnościami w Eklamot

Styczeń 2018

Spis treści

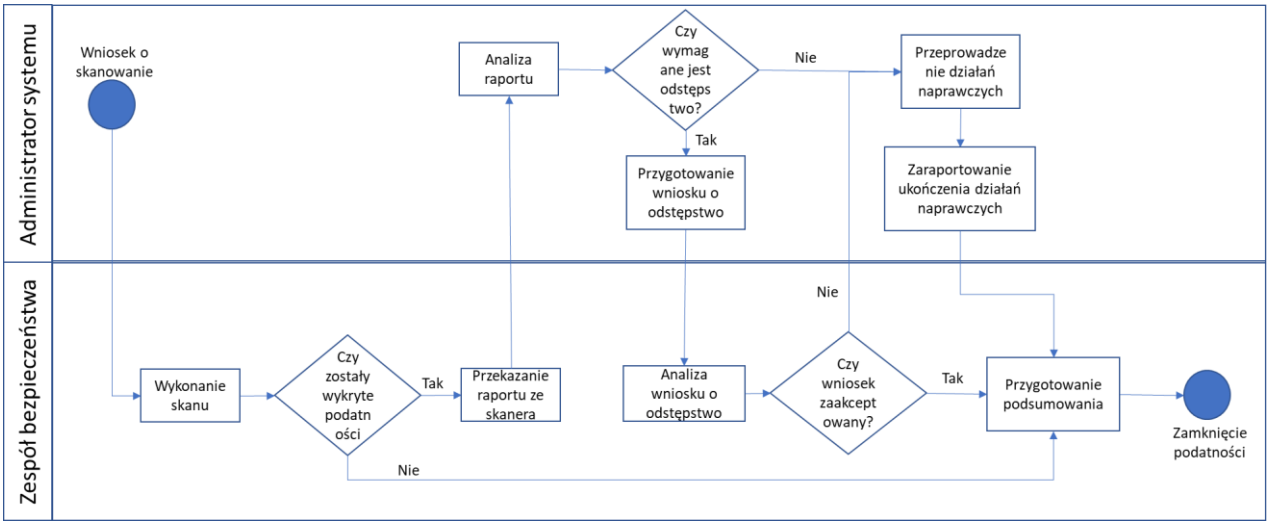
1. Wstęp

Celem niniejszego dokumentu jest przedstawienie procesu Zarządzania Podatnościami w eKlamot Niniejszy dokument zawiera opis procesu, w tym:

- cel procesu,
- przebieg procesu,
- strony zaangażowane w proces,
- KPI.

2. Zarządzanie podatnościami – cel i przebieg procesu

Celem procesu **Zarządzanie podatnościami** jest utrzymanie wysokiego poziomu bezpieczeństwa infrastruktury poprzez identyfikację znanych na rynku podatności a także raportowanie.



Przebieg procesu

1. **Przygotowanie wniosku o skanowanie –** w razie wystąpienia potrzeby skanowania, wniosek składa administrator systemu
2. **Przygotowanie i wykonanie skanu** narzędziem Nessus przez Zespół Bezpieczeństwa
3. **Czy zostały wykryte podatności? –** Weryfikacja, czy wskutek skanowania zostały wykryte podatności w ramach danego urządzenia.
4. Jeżeli nie wykryto podatności, skanowany system jest zgodny z wymaganiami bezpieczeństwa i po przygotowaniu podsumowania przez Zespół Bezpieczeństwa, proces ulega zamknięciu
5. **Przekazanie raportu ze skanera do administratora skanowanego systemu -** Jeżeli wskutek skanu wykryte zostały podatności, raport wygenerowany przez skaner przesyłany jest bezpośrednio do Administratora odpowiedzialnego za dany system
6. **Analiza raportu ze skanera** – raport ze skanera analizowany jest przez Administratora w celu identyfikacji, czy wykryte podatności nie są tzw. false positive, a więc są wykryte niesłusznie, najczęściej wskutek błędu technicznego lub też są to podatności, do których składano już wniosek o odstępstwo.

7. **Czy wymagane jest odstępstwo?** Punkt decyzyjny określający czy wymagane jest odstępstwo w ramach wykrytych podatności. Administrator systemu analizuje i decyduje, czy wymagane jest zgłoszenie wniosku o odstępstwo.

8. **Przygotowanie wniosku o odstępstwo** – jeśli administrator systemu zadecyduje o potrzebie odstępstwa, przygotowuje odpowiedni wniosek z uzasadnieniem, który wysyła do Zespołu Bezpieczeństwa

9. **Przeprowadzenie działań naprawczych -**– Jeżeli nie jest wymagane złożenie wniosku o odstępstwo, Administrator przystępuje do realizacji zaplanowanych działań naprawczych.

10. **Zaraportowanie ukończenia działań naprawczych -** Po zakończeniu działań, administrator systemu raportuje ich ukończenie zespołowi bezpieczeństwa.

11. **Analiza wniosku o odstępstwo** – dział bezpieczeństwa analizuje wniosek pod kątem merytorycznym w zakresie technologii, formułuje swoją opinię i decyduje o jego akceptacji lub odrzuceniu

12. **Czy wniosek o odstępstwo został zaakceptowany?** - Punkt decyzyjny określający, czy wniosek o odstępstwo został zaakceptowany przez Zespół Bezpieczeństwa. W przypadku gdy wniosek jest zaakceptowany, Zespół Bezpieczeństwa przygotowuje odpowiednie podsumowanie. Jeśli wniosek nie został zaakceptowany, administrator systemu musi podjąć działania naprawcze.

13. **Przygotowanie podsumowanie** – Zespół bezpieczeństwa przygotowuje odpowiednie podsumowanie w zależności czy proces zakończył się wdrożeniem działań naprawczych mających na celu wyeliminowanie wykrytych podatności lub też przyjęciem wniosku o odstępstwo.

3. Mierniki procesu (KPI)

Mierniki procesu mają za zadanie sprawdzać efektywność procesu oraz zidentyfikować tzw. *„wąskie gardła”* (ang. *bottleneck*), czyli elementy procesu, które znacząco obniżają jego efektywność:

Lp	Miernik (KPI)	Opis
1	Liczba wykrytych podatności w danym miesiącu	Liczba podatności, jakie zwraca skaner
2	Liczba złożonych wniosków o odstępstwo w danym miesiącu	Liczba wniosków złożonych przez administratorów
3	Liczba *false positive* w danym miesiącu	Liczba niesłusznie wykrytych przez skaner podatności (wskutek błędu technicznego lub też w przypadku, gdy jest to podatność, co do której zgłoszono już wcześniej wniosek o odstępstwo)
4	Średni czas zamknięcia podatności w danym miesiącu	Średni czas zamknięcia podatności liczony od momentu zakończenia skanu do przygotowania podsumowania przez Zespół Bezpieczeństwa