Politechnika Śląska

Sprawozdanie z modułu nr 1

BSKiST 2022/2023

Bezpieczeństwo sieci komputerowych i systemów teleinformatycznych

Kierunek: Informatyka

Członkowie zespołu:
Grzegorz Koperwas

Gliwice, 2022/2023

Spis treści

1 Wprowadzenie **2**
1.1 Zespół projektowy 2
1.2 Wprowadzenie 3
1.3 Rozwinięcie 3
1.4 Rodzaje ochrony przed zagrożeniami. 3

2 Podsumowanie i wnioski **4**

3 Spis literatury **5**

1 Wprowadzenie

1.1 Zespół projektowy

1. Grzegorz Koperwas :: Wszystko

1.2 Wprowadzenie

W internecie mamy do czynienia z wieloma rodzajami zagrożeń dla naszej infrastruktury teleinformatycznej, takimi jak:

- Wirusy i malware
- Ataki hakerskie
- Włamania i nieautoryzowane dostępy
- Phishing i oszustwa internetowe
- Awarie i błędy systemowe

Jednak w celu ochrony przed wyżej wymienionymi zagrożeniami, możemy skorzystać z wielu metod, oraz możemy oceniać stan infrastruktury ochronnej na wiele sposobów.

1.3 Rozwinięcie

1.4 Rodzaje ochrony przed zagrożeniami.

Istnieje wiele różnych, dobrze ze sobą współpracujących metod zabezpieczania naszej infrastruktury, lub wykrywania nieautoryzowanego dostępu, kiedy takowy nastąpi. Niektórymi z nich są:

1. **Ochrona oprogramowania oraz urządzeń przed wirusami i malware** - Zapewnienie wykrywania nieautoryzowanego oprogramowania gdy już się pojawi na komputerze jest jedną z podstawowych technik zabezpieczania systemów teleinformatycznych. Nawet jeżeli oprogramowanie nie jest nie bezpieczne dla naszego komputera, nadal konieczne jest jego wykrycie w celu zapobiegnięcia dalszego rozprzestrzeniania się takiego oprogramowania.

   Taką sytuacją może być wirus przeznaczony dla systemów `windows`, który może być przesyłany dalej przez serwer plików `samba` uruchomiony na systemie `GNU/Linux`. Programem mogącym zapobiegać takim sytuacjom jest na przykład `clamav`.

2. **Zabezpieczenie dostępu i identyfikacji użytkowników** - Odpowiednia konfiguracja oraz wykonanie systemu teleinformatycznego uniemożliwia nieautoryzowany dostęp do naszego systemu teleinformatycznego. Użycie autoryzacji opartej na hasłach jest powszechnie przyjętym

standardem, jednak posiada ono wiele wad wynikających z problemów spowodowanych obecnością członka gatunku *homo sapiens* pomiędzy klawiaturą (lub innym urządzeniem `HID`) a krzesłem bądź fotelem.

Z powyższego powodu, istnieje wiele alternatywnych rozwiązać, które wzmacniają tradycyjny proces autoryzacji hasłem przez dodanie nie stałych danych które użytkownik musi podać, lub poprzez wymagania od użytkownika posiadania określonych przedmiotów. Przykładami takich rozwiązań są:

- Google authenticator
- Autoryzacja przez kod przesyłany kanałem trzecim

3. Szyfrowanie danych i transmisji
4. Regularne aktualizacje
5. Monitoring i raportowanie incydentów bezpieczeństwa.

2 Podsumowanie i wnioski

- *Podsumowanie*
- *Wnioski*

3 Spis literatury