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

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.

2 Rozwinięcie

2.1 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. Na przykład przez wiadomość SMS lub e-mail.

Inne rozwiązania skupiają się na obowiązku posiadania przez użytkownika jakiejś informacji lub klucza. Może to być odcisk palca (biometria) lub klucz na karcie inteligentnej.

3. **Szyfrowanie danych i transmisji** - Wszystkie informacje wrażliwe powinny być przesyłane oraz przechowywane w sposób w który podmioty nieautoryzowane nie mają do nich dostępu.

4. **Regularne aktualizacje** - Regularne instalowanie aktualizacji bezpieczeństwa zabezpiecza nas przed znalezionymi lukami bezpieczeństwa. Dodatkowo nowoczesne rozwiązania w zakresie wytwarzania oprogramowania potrafią wyeliminować wiele błędów zanim zostaną dostarczone użytkownikowi.

5. **Monitoring i raportowanie incydentów bezpieczeństwa** - Monitorowanie naszej infrastruktury pozwala nam reagować jeśli nasze rozwiązania skupione na prewencji nie są sobie poradzić z nowymi rodzajami zagrożeń. Do tego celu mogą służyć różnego rodzaju zapory sieciowe nowego rodzaju.

2.2 Normy i standardy związane z bezpieczeństwem teleinformatycznym:

Istnieje wiele standardów umożliwiających łatwą i częstą ocenę odporności danego systemu teleinformatycznego na ataki i nieautoryzowany dostęp. Dodatkowo istnieją różne regulacje prawne które zmuszają podmioty do stosowania określonego poziomu zabezpieczeń przy przechowywaniu określonych informacji.

Niektórymi z nich są:

1. ISO 27001 - System Zarządzania Bezpieczeństwem Informacji
2. NIST SP 800-53 - Standardy Bezpieczeństwa w Systemach Rządu Federalnego Stanów Zjednoczonych
3. ISO 27032 - Zarządzanie Bezpieczeństwem Informacji w Środowisku Cyfrowym
4. RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679