**TEMAT: Mechanizmy wykrywania włamań**

Ważną grupę produktów podnoszących bezpieczeństwo systemów komputerowych stanowią programy pozwalające na wykrywanie włamań. W najnowszych rozwiązaniach granica pomiędzy systemami wykrywania włamań a zaporami sieciowymi zaczyna zanikać. Powstają systemy prewencji (ang. Intrusion Prevention System, IPS), które łączą filtrowanie ruchu sieciowego z aktywnym systemem wykrywania włamań

Systemy detekcji włamań są również związane z systemami sprawdzania integralności systemów plików. Rozwiązania tego typu nie zabezpieczają bezpośrednio systemów komputerowych, ale pomagają wykrywać niebezpieczeństwa związane z podejrzaną aktywnością w sieci czy nieautoryzowanymi próbami dostępu do systemów operacyjnych i zmian w plikach systemowych.

Działanie systemów detekcji włamań (ang. Intrusion Detection System, IDS) polega na monitorowaniu ruchu sieciowego i wykrywaniu zdarzeń, bądź sekwencji zdarzeń, które zgodnie ze zdefiniowanymi procedurami analizy są traktowane jako podejrzane. Mechanizmy reakcji na pozytywnie zidentyfikowane zagrożenie mogą być różne w zależności od poszczególnych systemów. Może to być bardzo prosta procedura polegająca jedynie na wysyłaniu informacji do administratora o wystąpieniu zdarzenia. Bardziej rozbudowane systemy IDS mogą podejmować o wiele bardziej złożone działania obronne, np. automatycznie blokować podejrzane adresy IP czy wyłączać atakowane usługi.

Pod względem sposobu działania systemów IDS można wyróżnić te, które działają w ramach sieci lokalnych (ang. Network Intrusion Detection System, NIDS) lub takie, które działają w obszarze systemów operacyjnych zainstalowanych na chronionym komputerze (ang. Host Intrusion Detection System, HIDS). Natomiast w zależności od metod wykrywania podejrzanych zdarzeń, systemy detekcji włamań można podzielić na działające na bazie sygnatur przypisanych do określonych rodzajów ataków lub takie, które potrafią wykrywać anomalie w ruchu sieciowym. Niestety, działania na bazie sygnatur znanych ataków są mało skuteczne, ponieważ rodzaje ataków mogą być bardzo różne, a najgroźniejsze z nich to takie, które dotychczas były nieznane i pojawiły się niedawno. Systemy IDS, które tylko wykrywają zagrożenie i informują o tym administratorów zwane są czasami systemami pasywnymi. Natomiast systemy, które mogą podejmować określone akcje blokujące ataki nazywane są systemami aktywnymi. Tego typu systemy uznawane są za bardziej skuteczne w ochronie systemów komputerowych.

Systemy detekcji włamań działają skutecznie pod warunkiem dostosowania ich konfiguracji do konkretnego systemu komputerowego i jego środowiska sieciowego. Jest to czynność czasochłonna i wymaga dużej kompetencji administratorów. Należy znaleźć kompromis, aby z jednej strony nie generować zbyt wielu fałszywych alarmów (ang. false positives), a z drugiej wykrywać jak największą ilość faktycznych groźnych prób włamania.

W systemie operacyjnym Windows dodatkowo zalecane jest stosowanie programów chroniących komputer przed wirusami. Tego typu programy można również zaliczyć do grupy systemów wykrywania włamań. Programy antywirusowe mogą działać na dwa sposoby: albo są uruchamiane przez system operacyjny lub administratora okresowo i sprawdzają wszystkie pliki w systemie, czy nie zostały zainfekowane, albo monitorują na bieżąco pliki używane przez wszystkie aplikacje. Wykrywanie wirusów obydwa się zwykle na podstawie tzw. sygnatur wirusów. Ta metoda jest skuteczna tylko wtedy, gdy producent oprogramowania już zidentyfikował wirusa, którym został zainfekowany komputer. Dlatego programy działające w ten sposób okresowo muszą uaktualniać bazę danych ze wzorcami sygnatur znanych wirusów. Istnieją również bardziej zaawansowane metody identyfikacji infekcji plików, tzw. metody heurystyczne, które pozwalają na wykrywanie nieznanych jeszcze wirusów [34]. Dla innych systemów operacyjnych również są dostępne programy antywirusowe, jednak z uwagi na małą ilość wirusów na tego typu platformy są one rzadko stosowane

|  |
| --- |
| **ZADANIE DOMOWE:**  Utwórz notatkę z lekcji w zeszycie. Skan bądź zdjęcie zeszytu proszę wysłać do dnia: **01.11.2020**na adres mailowy **k.pasiut@ptz.edu.pl**. **PRZEKONWETUJ PLIK TEKSTOWY DO FORMATU PDF!**  PLIK W FORMACIE **PDF**PROSZĘ DOKŁADNIE OPISAĆ:  **KLASA\_PRZEDMIOT\_IMIĘ\_NAZWISKO\_DATA LEKCJI**  Np.: 1B\_EUSIP\_JAN\_KOWALSKI\_16.09.2020  *W TEMACIE WIADOMOŚCI E-MAIL PROSZĘ WPISAĆ SWOJE NAZWISKO, KLASĘ ORAZ NAZWĘ PRZEDMIOTU*  **POWODZENIA☺** |