Wykład 8

Temat: Analiza ruchu sieciowego i obrona przed zagrożeniami z internetu

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Gdzie i jak analizujemy?

Gdzie:
- na brzegu sieci
- w poszczególnych gałęziach sieci
- bezpośrednio na serwerach

Jak:
- kopiowanie (mirroring) ruchu na oddzielną maszynę
- zapory sieciowe nowej generacji (CheckPoint, PaloAlto)
- węzły systemu IDS
- analiza statystyczna (sFlow, netFlow, itp)
- WAF (Web Application Firewall)

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

Czego szukamy?

- skanowania portów
- fałszywych (spoofing) i błędnych pakietów
- ruchu aplikacji których nie powinno być w naszej sieci
- pakietów zawierających określone frazy (password, login, itp)
- anomalii w ruchu (nagły wzrost ruchu do/z określonego hosta)
- pakietów zawierających kod znanego wirusa
- błędnych/dziwnych żądań HTTP

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Metody obrony

- automatyczne przerwanie złośliwej transmisji
- wpuszczanie i wypuszczanie tylko niezbędnego ruchu
- podział sieci na zewnętrzną i wewnętrzną
- separacja maszyn produkcyjnych i testowych
- częsta (codzienna) analiza logów

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Metody obrony

Dyskusja na temat tego co można odkryć analizując ruch sieciowy

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY