CSIRT GOV

ARAKIS GOV

ARAKIS GOV jest systemem wczesnego ostrzegania o zagrożeniach w sieci Internet, który powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej. System ten agreguje i przetwarza dane noszące znamiona potencjalnego ataku bądź złośliwego ruchu sieciowego, które koreluje z danymi już posiadanymi celem identyfikacji takich wskaźników jak m.in. unikalne adresy IP, porty, sygnatury czasowe oraz typ i metodologie zagrożeń.

ARAKIS GOV nie jest typowym systemem zabezpieczającym i w żadnym wypadku nie zastępuje funkcjonalności standardowych systemów ochrony sieci takich jak firewall, antywirus czy IDS/IPS.

Ze względu na swoją specyfikę może być z powodzeniem stosowany jako uzupełnienie w/w systemów, dostarczając informacji m.in. na temat:

1. Nowych zagrożeń (globalnych) pojawiających się w sieci Internet, m.in.:

    nowych typów ataków, obserwowanych z poziomu dużej liczby lokalizacji;

    trendów aktywności ruchu sieciowego na poszczególnych portach;

    trendów aktywności wirusów rozsyłanych pocztą elektroniczną;

2. Zagrożeń lokalnych związanych z konkretną, chronioną lokalizacją:

    zainfekowanych hostów w sieci wewnętrznej;

    nieszczelnej konfiguracji brzegowych systemów zaporowych;

    prób skanowania publicznej przestrzeni adresowej zarówno z Internetu jak i z sieci wewnętrznej

Główne funkcjonalności systemu ARAKIS GOV:

    analiza ruchu sieciowego w czasie rzeczywistym;

    analiza alarmów na podstawie wskaźników kompromitacji;

    mechanizm pułapek honeypot;

    wbudowany sandbox i analizator logów.

Ponadto zaimplementowane w systemie narzędzia umożliwiają między innymi porównanie statystyk ruchu sieciowego widzianego z poziomu chronionej lokalizacji z globalnym obrazem pochodzącym z wszystkich zainstalowanych sensorów oraz zobrazowanie geograficznej lokalizacji podejrzanego ruchu. Unikalną cechą systemu ARAKIS GOV jest przy tym fakt, że nie monitoruje on w żaden sposób treści informacji wymienianych przez chronioną instytucję z siecią Internet. Sondy systemu instalowane są bowiem poza chronioną siecią wewnętrzną instytucji, po stronie

sieci Internet. W chwili obecnej sensory systemu zainstalowane są w ponad 140 instytucjach administracji publicznej oraz podmiotach wchodzących w skład tzw. Infrastruktury krytycznej.