

System ARAKIS-GOV



ARAKIS-GOV jest systemem wczesnego ostrzegania o zagrożeniach w sieci Internet. System ten jest efektem współpracy Departamentu Bezpieczeństwa Teleinformatycznego ABW oraz działającego w ramach NASK zespołu CERT Polska. ARAKIS-GOV powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych **administracji państwowej** w wyniku rozszerzenia stworzonego przez CERT Polska systemu ARAKIS o dodatkową funkcjonalność.

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 jednak na swoją specyfikę może być z powodzeniem stosowany jako uzupełnienie w/w systemów, dostarczające informacji na temat:

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

- nowo-wykrytych samo-propagujących się zagrożeń typu worm;
- 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:

- braku aktualnych szczepionek antywirusowych;
- zainfekowanych hostów w sieci wewnętrznej;
- nieszczelnej konfiguracji brzegowych systemów zaporowych;
- prób skanowania publicznej przestrzeni adresowej zarówno z Internetu jak i z sieci wewnętrznej

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 60 urzędach szczebla centralnego i jednostkach samorządu terytorialnego.

System ARAKIS-GOV został doceniony przez

Fundację Polskiego Godła Promocyjnego, która realizuje

Program Promocyjny "Teraz Polska", przyznając w roku 2010 nagrodę

Godła „Teraz Polska” w kategorii

„Przedsięwzięć Innowacyjnych”.

Podmioty zainteresowane dołączeniem do projektu proszone są o przesłanie stosownej informacji na adres arakis.dbti@abw.gov.pl . Udział w projekcie ARAKIS-GOV jest **bezpłatny**.

A

A⁺

A⁺⁺



PDF

[Wersje dokumentu](#)