ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 294, Elektrotechnika 35
RUTJEE, z. 35 (2/2016), kwiecień-czerwiec 2016, s. 79-87

**Maksymilian BURDACKI**[1]
**Paweł DYMORA**[2]
**Mirosław MAZUREK**[3]

# PROGRAMY ANTYWIRUSOWE TYPU KLIENT/CHMURA – PERSPEKTYWY ROZWOJU, WYDAJNOŚĆ, ZAGROŻENIA

W artykule omówiono działanie oprogramowania antywirusowego typu klient/chmura oraz różnice pomiędzy standardowym oprogramowaniem antywirusowym działającym w oparciu o „ciężkiego klienta". Przedstawiono perspektywy rozwoju oprogramowania tego typu. W części badawczej porównano działanie obu typów programów. Dokonano oceny wpływu oprogramowania antywirusowego na wykorzystanie pamięci RAM, użycie procesora oraz wpływu na szybkość działania systemu i wykrywalności złośliwego oprogramowania przez testowane programy antywirusowe.

**Słowa kluczowe:** architektura klient/chmura, program antywirusowy, sygnatury wirusowe, chmury obliczeniowe.

## 1. Wprowadzenie

W ostatnich latach nastąpił gwałtowny wzrost ilości złośliwego oprogramowania, co spowodowało, że dotychczasowe rozwiązania antywirusowe przestały być wystarczające. Producenci oprogramowania antywirusowego zaczęli zastanawiać się nad nowymi technikami, które gwarantowałyby bezpieczeństwo użytkowników korzystających z sieci. Efektem ich prac było stworzenie nowego typu oprogramowania antywirusowego opartego na architekturze klient/chmura. Działanie takiego rozwiązania znacznie różni się od standardowych programów tego typu. Oprogramowanie typu klient/chmura pracuje z metadanymi (informacjami o pliku), które są przesyłane do chmury, a nie z obiektami w formie plików. Niniejszy artykuł jest próbą oceny efektywności tego typu oprogramowania w odniesieniu do tradycyjnych programów antywirusowych .

[1] Autor do korespondencji: Maksymilian Burdacki, Politechnika Rzeszowska, maxb931@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Katedra Energoelektroniki, Elektroenergetyki i Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

## 2. Oprogramowanie antywirusowe architektury typu klient/chmura - charakterystyka

Określenie „chmura antywirusowa" odnosi się do infrastruktury, która jest używana przez firmę antywirusową w celu przetwarzania informacji uzyskanych z komputerów osób korzystających z określonego produktu, aby zidentyfikować nowe, nieznane zagrożenia. Technologie używane do przechowywania i przetwarzania danych użytkownika działają w tle. Oprogramowanie antywirusowe wysyła żądanie do chmury, aby sprawdzić czy jest tam dostępna jakakolwiek informacja dotycząca określonego programu, działania, linku czy zasobu. Odpowiedź wygląda następująco: „tak, jest dostępna informacja" lub „nie, nie ma dostępnej informacji". System aktualizacji zakłada jednokierunkową interakcję pomiędzy firmą antywirusową i użytkownikiem: od producenta oprogramowania antywirusowego do użytkownika. Nie ma informacji zwrotnych od użytkownika, co powoduje, że nie jest możliwe natychmiastowe zidentyfikowanie podejrzanego działania lub uzyskanie informacji o rozprzestrzeniającym się zagrożeniu lub jego źródłach [1].

W przeciwieństwie do systemu aktualizacji podejście oparte na chmurze jest dwukierunkowe. Komputery podłączone do chmury za pomocą centralnego serwera informują chmurę o źródłach infekcji, a także o podejrzanych działaniach, które zostały wykryte. Po przetworzeniu informacji, stają się one dostępne dla innych komputerów, które są podłączone do chmury. W rzeczywistości użytkownicy mają możliwość dzielenia się informacjami za pośrednictwem infrastruktury firmy antywirusowej dotyczącymi ataków uruchomionych przeciwko nim i źródłach tych ataków. W wyniku otrzymano zintegrowaną, rozproszoną intelektualnie sieć antywirusową działającą jako całość. Główną różnicą pomiędzy chmurą i istniejącymi technologiami antywirusowymi jest obiekt, który został wykryty. Poprzednie generacje technologii takie jak np. sygnatury pracowały z obiektami w formie plików, natomiast chmura antywirusowa pracuje z metadanymi. Metadane są to informacje o pliku zawierające: unikalny identyfikator pliku (funkcja hash), dane o tym, w jaki sposób plik przedostał się do systemu, jak się zachowywał itp. Nowe zagrożenia są identyfikowane w chmurze używając metadanych, chociaż pliki same w sobie nie są właściwie przesyłane do chmury do wstępnej analizy [1, 4].

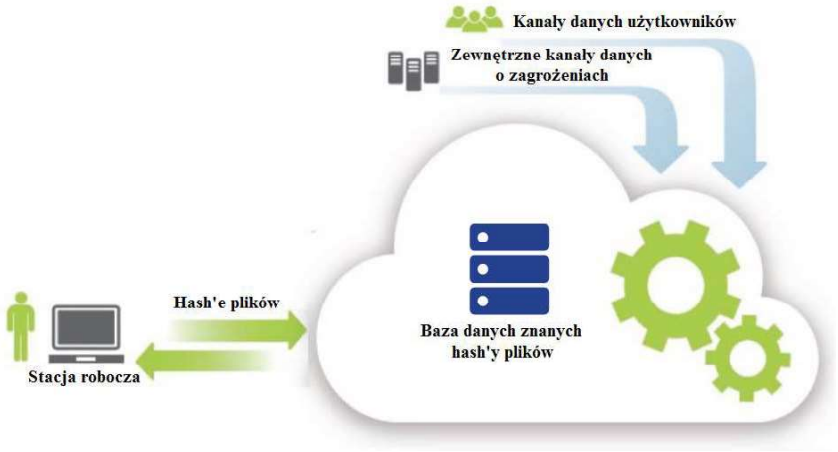
## 3. Architektura „ciężkiego klienta"

Architektura „ciężkiego klienta" tradycyjnych produktów antywirusowych opiera się na modułach zajmujących dużą ilość pamięci dyskowej na punktach końcowych. Zadaniem tych modułów jest porównywanie podejrzanych plików z sygnaturami zagrożeń. Tego typu rozwiązanie posiada wady, gdyż spowalnia szybkość przetwarzania punktu końcowego poprzez skanowanie w poszukiwaniu złośliwego oprogramowania i porównywanie sygnatur, co zmniejsza dodat-

kowo wydajność, denerwuje użytkowników i w części przypadków powoduje wyłączenie oprogramowania antywirusowego przez użytkownika. Tysiące nowych sygnatur są wysyłane do punktów końcowych (średnio 5 MB na punkt końcowy każdego dnia), co pochłania przepustowość łącza i wymaga monitorowania przez administratorów systemu.

Architektura typu klient/chmura fundamentalnie zmienia tę sytuację. Na punkcie końcowym potrzebny jest tylko bardzo lekki klient, który znajduje nowe pliki i tworzy hash'e (sygnatury) tych plików. Hash'e są wysyłane do serwera opartego na chmurze i porównywane z rozbudowaną bazą danych sygnatur. Odpowiedzi są wysyłane z powrotem do punktu końcowego [2, 5].

Na Rys. 1. przedstawiono schemat architektury oprogramowania antywirusowego typu klient/chmura.




Rys. 1. Schemat architektury oprogramowania antywirusowego typu klient/chmura, na podstawie [2]

Fig. 1. The architecture of the client/cloud antivirus, based on [2]

Architektura typu klient/chmura ma ogromną przewagę nad tradycyjnymi produktami antywirusowymi. Niesie ona ze sobą następujące korzyści:

- Na urządzeniu końcowym wykonywane jest niewiele zadań, dzięki czemu jego wydajność nie zmniejsza się.
- Nie ma znacznego wpływu na użycie pasma lub wydajność sieci, ponieważ tylko kilka hash'y w danym systemie jest wymienianych przez sieć (zwykle około 120 KB dziennie) zamiast tysięcy nowych sygnatur zagrożeń.
- System oparty na chmurze dysponuje ogromną bazą danych sygnatur i używa serwerów o dużej mocy obliczeniowej do porównywania wzorców, co powoduje, że ten proces jest bardziej kompletny i szybszy.

- System oparty na chmurze otrzymuje w czasie rzeczywistym dane dotyczące zagrożeń od laboratoriów testowych, producentów oprogramowania antywirusowego, tysięcy przedsiębiorstw i milionów użytkowników, więc zagrożenia typu zero-day mogą zostać zablokowane tak szybko jak tylko zostaną zidentyfikowane.
- Administratorzy systemów nie muszą poświęcać czasu na instalowanie „ciężkiego klienta" lub aktualizowanie sygnatur na każdym urządzeniu końcowym.

Programy antywirusowe, których działanie oparte jest o ciężkiego klienta są całkowicie przestarzałe. Architektura klient/chmura jest jedynym sposobem, aby dopasowywanie sygnatur w czasie rzeczywistym stało się praktyczne i efektywne [2].

## 4. Porównanie oprogramowania

Przeprowadzone badania miały na celu porównanie oprogramowania antywirusowego architektury typu klient/chmura oraz standardowego oprogramowania antywirusowego typu „ciężki klient". Przeprowadzono je na wirtualnej maszynie stworzonej w programie Oracle VM VirtualBox.

W przeprowadzanych testach porównano wpływ poszczególnych programów antywirusowych na różne aspekty działania maszyny wirtualnej. W badaniach wykorzystano następujące oprogramowanie antywirusowe:

- Panda Free Antivirus 16 (program typu klient/chmura),
- Trend Micro Internet Security 10 (program typu klient/chmura),
- BullGuard Internet Security 16 (program działający w oparciu o „ciężkiego klienta"),
- Avast Internet Security 11 (program działający w oparciu o „ciężkiego klienta").

### 4.1. Pamięć RAM oraz użycie procesora

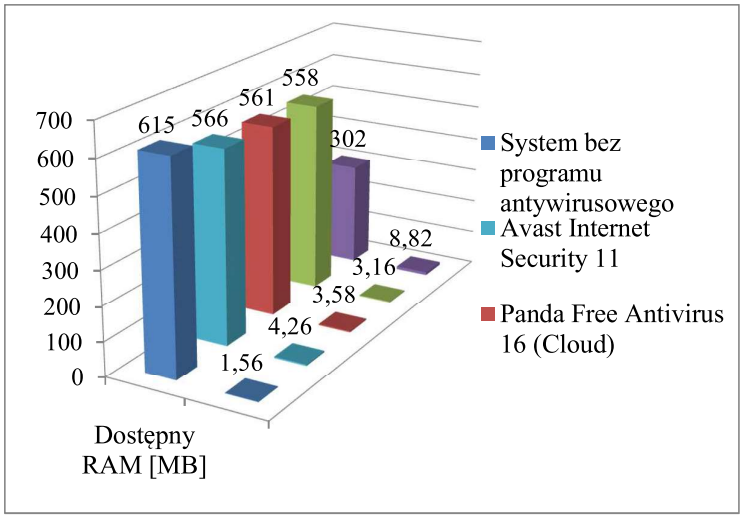
W tej części testów skupiono się na sprawdzeniu wpływu tych aplikacji na wykorzystanie pamięci RAM oraz użycie procesora. Badania zostały przeprowadzone zarówno w czasie działania jałowego jak i podczas całkowitego skanowania systemu. Do przeprowadzenia badań wykorzystano systemowe narzędzie PERFMON, które pozwala na monitorowanie i zapisywanie do pliku parametrów komputera. W czasie przeprowadzanych testów parametry zapisywano do pliku co 5 sekund.

#### 4.1.1. Wariant 1 - praca jałowa

Badania były przeprowadzano przez okres 5 minut. W tym czasie na maszynie nie były wykonywane żadne operacje, aby otrzymane wyniki były wiary-

godne. Trzy spośród czterech testowanych programów antywirusowych wykorzystywały podobną ilość pamięci RAM. W przeprowadzonym teście najlepiej wypadło oprogramowanie Avast Internet Security. Ilość dostępnej pamięci RAM na systemach z zainstalowanymi programami typu klient/chmura była o tylko kilka MB mniejsza niż w przypadku systemu z zainstalowanym oprogramowaniem firmy Avast. Najgorszy wynik został osiągnięty na maszynie z zainstalowanym oprogramowaniem BullGuard Internet Security. Był on o 264 MB gorszy w stosunku do wyniku otrzymanego na maszynie z zainstalowanym oprogramowaniem firmy Avast. Badane programy antywirusowe obciążały procesor w niewielkim stopniu, wahającym się od 3% do 8,82%.

Na Rys. 2. przedstawiono porównanie ilości dostępnej pamięci RAM oraz średnie użycie procesora w systemie podczas działania jałowego dla wszystkich testowanych programów.




Rys. 2. Porównanie ilości dostępnej pamięci RAM oraz użycia procesora w systemie w czasie działania jałowego dla wszystkich testowanych programów

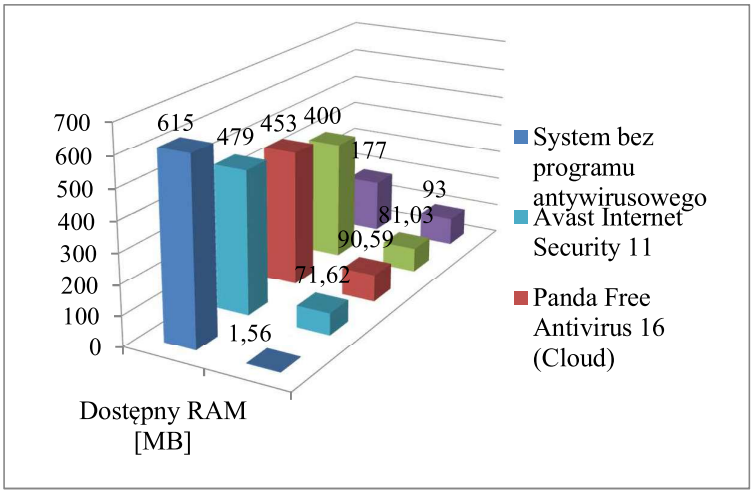
Fig. 2. Comparing the amount of available RAM and CPU usage in the idle system for all tested programs

### 4.1.2. Wariant 2 - całkowite skanowanie maszyny

Czasy trwania testów poszczególnych programów antywirusowych były różne. Było to spowodowane zróżnicowanym czasem potrzebnym do przeprowadzenia całkowitego skanowania maszyny za pomocą testowanych programów. Podczas skanowania na maszynie nie były wykonywane żadne operacje, aby otrzymane wyniki były wiarygodne.

Dostępna pamięć RAM była różna w zależności od używanego programu antywirusowego. Najwięcej dostępnej pamięci było w czasie skanowania za pomocą programu Avast Internet Security. Programy Panda Free Antivirus oraz Trend Micro Internet Security osiągnęły nieco gorsze wyniki. Najmniej dostępnej pamięci było w trakcie skanowania za pomocą programu BullGuard Internet Security. Program ten obciążał pamięć RAM w największym stopniu.

Na Rys. 3 przedstawiono porównanie ilości dostępnej pamięci RAM oraz wykorzystania procesora w czasie skanowania maszyny przy użyciu testowanych programów antywirusowych. Wszystkie badane programy antywirusowe znacznie obciążały procesor w trakcie skanowania systemu. Program Avast Internet Security wykorzystywał procesor w najmniejszym stopniu około 71,62%. Największe obciążenie procesora zostało zanotowane podczas skanowania za pomocą programu BullGuard Internet Security 93 %.




Rys. 3. Porównanie ilości dostępnej pamięci RAM oraz wykorzystania procesora w czasie skanowania maszyny w trybie jałowym

Fig. 3. Comparing the amount of available RAM and CPU utilization during scanning process in the idle system

## 4.2. Badania wpływu oprogramowania antywirusowego na szybkość działania systemu

Do oceny wpływu obecności w systemie programów antywirusowych przeprowadzanych w trakcie działania jałowego tj. czystego, bez zainfekowanych plików przeprowadzono szereg testów, uwzględniających m. in. czas uruchomienia systemu, czas kopiowania folderu testowego (o pojemności 2 GB), czas archiwizacji przykładowego folderu (300 MB, program Easy 7-Zip), czas rozpa-

kowywania archiwum testowego (program Easy 7-Zip), czas instalacji pakietu biurowego Microsoft Office 2003 (standardowe ustawienia), czy czas trwania całkowitego skanowania systemu. Dla każdego programu zostały wykonane 3 pomiary i na podstawie tych wartości zostały obliczone średnie. W Tab. 1 przedstawiono szczegółowe wyniki przeprowadzonych badań.

Tabela 1. Porównanie szybkości działania systemu

Table 1. Comparison of the speed of the system

| | **System bez programu antywirusowego** | **Panda Free Antivirus 16** | **Trend Micro Internet Security 10** | **BullGuard Internet Security 16** | **Avast Internet Security 11** |
|---|---|---|---|---|---|
| Czas uruchomienia systemu [s] | 30 | 57 | 43 | 50 | 53,67 |
| Czas kopiowania folderu testowego – działanie jałowe [min:s] | 4:25 | 6:21 | 5:23 | 5:38 | 4:50 |
| Czas archiwizacji folderu testowego [min:s] | 2:26 | 2:49 | 2:40 | 2:38 | 2:30 |
| Czas rozpakowywania archiwum testowego [s] | 21 | 32 | 22,33 | 28 | 21 |
| Czas instalacji pakietu biurowego Microsoft Office 2003 [min:s] | 2:42 | 4:25 | 4:24 | 4:24 | 3:38 |
| Czas całkowitego skanowania maszyny [min:s] | - | 37:29 | 30:46 | 46:12 | 13:09 |

Producenci oprogramowania antywirusowego typu klient/chmura zapewniają, że programy tego typu w dużo mniejszym stopniu wpływają na wydajność komputera w porównaniu ze standardowymi programami antywirusowymi. Badania, których wyniki zostały zaprezentowane nie do końca potwierdzają te zapewnienia. W testach czasowych zdecydowanie najlepiej poradził sobie program Avast Internet Security. Programy BullGuard Internet Security oraz Trend Micro Internet Security w testach czasowych wypadły nieco gorzej od programu firmy Avast. Zdecydowanie najgorsze wyniki zostały otrzymane na maszynie z zainstalowanym programem Panda Free Antivirus.

## 4.3. Badania wykrywalności złośliwego oprogramowania

Do oceny wykrywalności złośliwego oprogramowania przeprowadzano testy mające na celu sprawdzenie czasu wykrycia i usunięcia zainfekowanych plików. Uwzględniono również wpływ braku dostępu do Internetu na działanie oprogramowania antywirusowego typu klient/chmura. Przeprowadzone testy obejmowały badanie wykrywalności złośliwego oprogramowania (zainfekowano

300 plików), liczby usuniętych zainfekowanych plików, wpływ braku dostępu do Internetu na wykrywalność zagrożeń oraz liczbę usuniętych zainfekowanych plików. W Tab. 2 przedstawiono wyniki przeprowadzonych badań.

Tabela 2. Porównanie skuteczności działania programów antywirusowych

Table 2. Comparison of the effectiveness of anti-virus software

| | **Panda Free Antivirus 16** | **Trend Micro Internet Security 10** | **BullGuard Internet Security 16** | **Avast Internet Security 11** |
|---|---|---|---|---|
| Liczba wykrytych zagrożeń | 235 | 252 | 198 | 354 |
| Liczba usuniętych zainfekowanych plików | 199 | 193 | 188 | 186 |
| Liczba wykrytych zagrożeń bez dostępu do Internetu (tylko programy klient/chmura) | 107 | 38 | - | - |

Badania mające na celu sprawdzenie wykrywalności złośliwego oprogramowania i liczby usuniętych szkodliwych plików nie wyłoniły jednego programu, który poradził sobie z tymi zadaniami najlepiej. Program Avast Internet Security wykrył zdecydowanie najwięcej zagrożeń spośród testowanych programów. Jednak ilość wykrytych zagrożeń nie pokrywa się z liczbą usuniętych zainfekowanych plików. W tym teście najlepiej wypadł program Panda Free Antivirus, który usunął najwięcej szkodliwych plików. Badano również wpływ braku dostępu do Internetu na oprogramowanie antywirusowe klient/chmura. Z przeprowadzonego testu wynika, że brak dostępu do sieci znacznie zmniejsza skuteczność wykrywania złośliwego oprogramowania przez programy antywirusowe działające w oparciu o chmurę.

## 5. Podsumowanie

Przeprowadzone testy wykazały, że programy działające w oparciu o chmurę mają niewielki wpływ na wydajność komputera, co nie jest regułą w przypadku programów, które korzystają z tzw. „ciężkiego klienta”. Istnieją jednak programy, które pomimo tego, że nie korzystają z chmury antywirusowej w małym stopniu obciążają zasoby komputera. Oprogramowanie antywirusowe działające w oparciu o architekturę klient/chmura nie jest bez wad. Brak dostępu do Internetu powoduje znaczne zmniejszenie wykrywalności złośliwego oprogramowania przez tego typu programy. Taka sytuacja nie występuje w przypadku programów, które wykrywają wirusy na podstawie sygnatur pobieranych na dysk komputera.

Programy antywirusowe działające w oparciu o architekturę klient/chmura stanowią poważną alternatywę dla programów korzystających z tzw. „ciężkiego klienta”. Takie cechy jak duża szybkość działania, mały wpływ na wydajność

systemu oraz wysoka wykrywalność złośliwego oprogramowania mogą zachęcić wielu użytkowników do korzystania z tego typu oprogramowania. Poprzez gromadzenie i przetwarzanie danych od każdego użytkownika sieci, chmura jest silnym systemem ekspertowym zaprojektowanym do analizy działalności cyberprzestępczej. Dane potrzebne do blokowania ataków są dostarczane do wszystkich uczestników sieci chmury, co pomaga zapobiegać kolejnym infekcjom. Maksymalna ochrona może zostać osiągnięta jednak poprzez połączenie obecnie panujących technologii bezpieczeństwa z systemami antywirusowymi opartymi na chmurze.

## Literatura

[1] https://securelist.com/analysis/publications/36321/the-antivirus-weather-forecast-cloudy/ [Dostęp: 20.05.2016]

[2] https://www.webroot.com/shared/pdf/reinventing-antivirus.pdf [Dostęp: 25.05.2016]

[3] Ziarek M.: Oprogramowanie antywirusowe w chmurze. Biznes benchmark magazyn, nr 3/10/2013, str. 54-55.

[4] Lehtinen R., Russell D., Gangemi G.T.: Podstawy ochrony komputerów. Helion, Gliwice 2007.

[5] Harley D., Slade R., Gattiker U. E.:Wirusy cała prawda: Zrozum i powstrzymaj szkodliwe oprogramowanie. Translator, Warszawa 2003.

## CLIENT/CLOUD ARCHITECTURE ANTIVIRUS SOFTWARE - DEVELOPMENT PROSPECTS, PERFORMANCE, RISKS

**S u m m a r y**

The presented article describes issues referring to cloud computing, history of antivirus software, kinds of malicious software and client/cloud antivirus software. The aim of the thesis is comparison of client/cloud antivirus software and standard “fat client” antivirus software. Two “fat client” antiviruses and two client/cloud antiviruses were compared. Influence on system performance and malicious software detection rate were checked during testing. After the research it was possible to draw conclusions about each type of antivirus software.

**Keywords:** client/cloud antivirus software, cloud computing, computer viruses.

DOI: 10.7862/re.2016.12

*Tekst złożono w redakcji:* maj 2016
*Przyjęto do druku:* czerwiec 2016