ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Paweł TAMA, Ireneusz J. JÓŹWIAK, Jacek GRUBER
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

BEZPIECZEŃSTWO I NIEZAWODNOŚĆ SIECI FIRMOWEJ DUŻEJ SKALI – STUDIUM PRZYPADKU

Streszczenie. Celem artykułu jest omówienie ochrony antywirusowej w korporacji. Zadaniem tej ochrony ma być zabezpieczenie użytkowników komputerów i systemów informatycznych IT oraz systemów produkcyjnych przed złośliwym oprogramowaniem i hakerami. Opisano, jak wybierać program antywirusowy, oraz wskazano najszybszą ścieżkę wdrożenia takiego oprogramowania. Omówiono narzędzie, które pozwala utrzymać bezpieczeństwo sieci firmowej lub korporacyjnej na wysokim poziomie niezawodnościowym. Zaproponowano metodę ułatwiającą wdrożenie systemu przy uwzględnieniu zasad grup dostępnych w usłudze katalogowej Active Directory Domain Services.

Słowa kluczowe: program antywirusowy, usługa katalogowa, zasady grup, systemowy firewall, narzędzie Nagios.

SAFETY AND RELIABILITY OF LARGE-SCALE CORPORATE NETWORKS – CASE STUDY

Summary. The aim of the study is to discuss the corporate anti-virus protection. The purpose of this protection is to protect the users of computers and information systems, IT and production systems from malicious software and hackers. Method of making a choice of anti-virus program and a description of the quickest path software implementation of such software are explained in this article. Description of tools that allows you to maintain the security of the corporate network or enterprise at the level high of reliability, was also included. The method facilitates the implementation of the system, taking into account the principles of groups available in the Active Directory Domain Services has also been presented.

Keywords: antivirus, catalog services, active directory domain services, group policy, system firewall, Nagios utility.

1. Wstęp

Istnieją różne sposoby, dzięki którym można zabezpieczyć sieci korporacyjne lub firmowe i ich zasoby. W tym celu należy zastosować mechanizmy bezpieczeństwa dostarczane przez różnych producentów. W niniejszym artykule skoncentrujemy się na platformie operacyjnej i sieciowej Microsoft, ponieważ jest ona dominująca w infrastrukturze zasobów IT i systemów produkcyjnych korporacji z rozważanego tutaj studium przypadku. Cała ta infrastrukturalna platforma jest oparta na systemie operacyjnym Microsoft Windows Serwer 2008 R2. Rozważana platforma korporacyjna używa usługi katalogowej Active Directory Domain Services. W publikacji znajduje się studium przypadku migracji komputerów domeny do środowiska antywirusowego w dużej korporacji, liczącej ponad 10 tys. pracowników. Korporacja jest jednym ze światowych dostawców systemów bezpieczeństwa i kontroli, technologii elektronicznych, mechanicznych i mechatronicznych do układów hamulcowych, układów stabilizacji i automatycznych skrzyń przekładniowych dla światowych producentów samochodów ciężarowych, naczep i autobusów.

Głównym źródłem wiedzy do opisu rozwiązań, które dalej opisano w artykule, są doświadczenia zawodowe jednego z Autorów oraz znajomość innych spotykanych rozwiązań i technologii poznanych przez wszystkich Autorów. Tak więc nadal nie ma usystematyzowanej i zebranej wiedzy, której zastosowanie umożliwiłoby w prosty i szybki sposób migrację systemów informatycznych do rozwiązań antywirusowych. Istnieje wielu producentów oprogramowania antywirusowego, lecz żaden z nich nie podaje sposobu aktualizacji oprogramowania w dużych sieciach komputerowych. Autor książki [1] w bardzo prosty sposób opisuje sposób działania usługi katalogowej *active directory*. Producenci oprogramowania antywirusowego opracowują i udostępniają instrukcje związane z konfiguracją programów antywirusowych. Celem Autorów niniejszej pracy jest:

- podanie prostego i szybkiego sposobu, który można wykorzystać podczas migracji systemów informatycznych do nowych rozwiązań antywirusowych dostępnych na rynku,
- sposób zabezpieczenia przed zagrożeniami oraz utrzymania na wysokim poziomie niezawodnościowym systemów informatycznych.

2. Studium przypadku

Jednym z kluczowych mechanizmów zapewniających bezpieczeństwo w systemie operacyjnym Windows Serwer 2008 jest zapora Windows Firewall. Zapora hosta z analizą stanu połączeń zezwala na ruch w sieci lub blokuje go zależnie od konfiguracji określającej reguły dotyczące zezwoleń i blokad. Windows Firewall ma więc za zadanie zabezpieczyć zasoby hostów i infrastruktury przed złośliwymi użytkownikami i szkodliwym

oprogramowaniem. Gdy prawidłowo skonfigurowano usługę Windows Firewall, ustawiono odpowiednie reguły i zabezpieczono ruch przychodzący i wychodzący, to jest zapewniony dość duży poziom ochrony zasobów i platformy IT korporacji. Sieć korporacyjna, mająca setki serwerów, musi być zatem zabezpieczona za pomocą wymienionych powyżej mechanizmów. Należy pamiętać, że niezależnie od zastosowanych mechanizmów zabezpieczeń pozostaje pewne ryzyko szczątkowe podatności na ataki będące konsekwencją infekowania hostów wirusami komputerowymi. Naszym celem jest przede wszystkim jego minimalizowanie. Odpowiedź na pytanie, czy w przypadku prawidłowo i efektywnie stosowanych zapór systemowych ryzyko jest już odpowiednio małe, jest niestety negatywna. Posiadanie systemu operacyjnego z firewallem zwiększa bezpieczeństwo, ale nie powoduje, że bezpieczeństwo sieci firmowej jest na odpowiednio wysokim poziomie [2].

Bardzo ważnym elementem, który odpowiada za bezpieczeństwo w firmie, jest ochrona antywirusowa. Jest ona bardzo ważna, gdyż bez programu usuwającego szkodliwe oprogramowanie korporacja musi przygotować się na duże straty materialne oraz bardzo wysokie ryzyko związane z brakiem ochrony kluczowych serwerów i innych ważnych zasobów oprogramowania i infrastruktury IT, hostów i sieci przemysłowych. W niektórych przypadkach może się to skończyć bankructwem całej korporacji lub firmy. Dobitnym przykładem konsekwencji braku zabezpieczenia antywirusowego jest zaatakowanie komisariatu policji przez szkodliwe oprogramowanie, którego celem było zniszczenie danych policyjnych. Po ataku funkcjonariusze stracili wszystkie ważne pliki oraz zostały uszkodzone lokalne policyjne bazy danych. Nie udało się odzyskać danych, lecz w konsekwencji w celu uchronienia się przed tego typu zdarzeniami w przyszłości komisariat wyposażono w najnowsze zabezpieczenia antywirusowe. Jest to tylko jeden z wielu przykładów, w którym z powodu zbagatelizowania zasad bezpieczeństwa ponosi się potężne straty.

Do ważnych decyzji należy wybór producenta oprogramowania antywirusowego, które powinno się zastosować. Podczas wyboru najlepiej posłużyć się strategicznymi analizami firmy Gartner [3]. Obszar działalności tej firmy jest bardzo duży. Skupmy się na bezpieczeństwie i zarządzaniu ryzykiem. Aby znaleźć najlepsze rozwiązanie dla firmy, należy skorzystać z tzw. Gartnet Magic Quadrant dla ochrony antywirusowej [4]. Wykres przedstawiony na rysunku 1 jest podzielony na cztery części: 1) NichePlayers, 2) Visionaries, 3) Challengers, 4) Leaders.

Rys. 1. Magiczny kwadrat Gartnera obrazujący producentów oprogramowania antywirusowego
Fig. 1. Gartner Magic Quadrant showing anti-virus vendors
Źródło: Gartner (January 2014) [3].

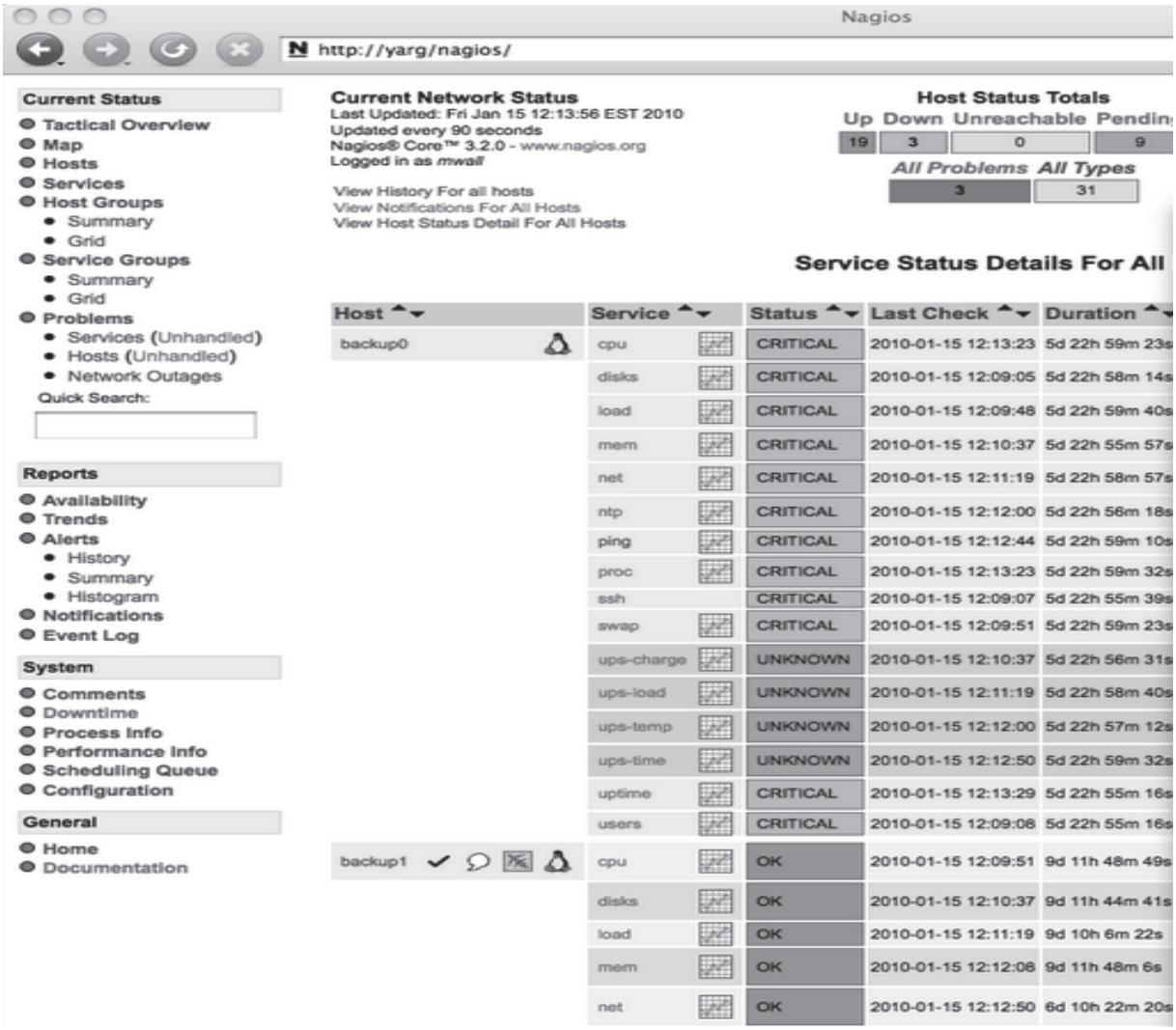
Przy wybieraniu programu antywirusowego powinniśmy skupić się na I ćwiartce dotyczącej producentów (LEADERS). Zgodnie z rysunkiem 1 pięciu producentów oprogramowania antywirusowego znajduje się w czołówce. Powstaje problem, w jaki sposób zabezpieczyć korporację, w której liczba stacji roboczych i serwerów jest rzędu kilku lub kilkunastu tysięcy. Podstawową zasadą rozwiązania tej kwestii, jaką powinniśmy się kierować, jest zabezpieczenie kluczowych dla firmy lub korporacji serwerów, np. serwerów pocztowych i serwerów SQL. Serwery plików są również ważne, gdyż przechowują dane pracowników. W zasadzie oprogramowanie antywirusowe jest w stanie ochronić wszystkie zasoby platformy IT oraz zapewnić odpowiedni poziom jej bezpieczeństwa. Po podjęciu decyzji o zastosowaniu technologii i rozwiązania danego producenta rozwiązanie należy

wdrożyć. Zgodnie z rysunkiem 1 najlepszym wyborem jest program antywirusowy firmy McAfee. Podczas wdrażania nowego oprogramowania wszelkie obowiązki z tym związane powinny być realizowane przez administratora. Nie można tym zadaniem obciążać użytkowników IT i systemów technologicznych. Wszystkie procedury wdrożeniowe powinny wykonać się automatycznie, bez ingerencji użytkownika. Bazy danych sygnatur wirusów muszą być stale aktualizowane, gdyż cały czas powstają nowe zagrożenia.

Najszybszy sposób wdrożenia oprogramowania antywirusowego w dużej firmie lub w korporacji liczącej ponad 10 tys. pracowników opiera się na zasadach grup. Jeśli firma ma oprogramowanie antywirusowe, administrator powinien za pomocą skryptów logowania użytkownika GPO (Group Policy Object) usunąć dotychczas działający program antywirusowy ze wszystkich komputerów. Następnie należy zaplanować wdrożenie nowego programu, uwzględniając wszystkie lokalizacje w firmie lub w korporacji. W omawianym tu przypadku korporacja działa na wszystkich kontynentach i w wielu lokalizacjach. Jednym z najczęstszych sposobów instalacji oprogramowania na komputerach końcowych jest wykorzystanie skryptu logowania użytkownika przez GPO. Gdy użytkownik zaloguje się na komputerze, program zostanie automatycznie zainstalowany. Później administrator będzie mógł zarządzać nim bezpośrednio z poziomu konsoli antywirusowej. Po ukończeniu dystrybucji oprogramowania należy sprawdzić, czy sygnatury baz wirusów są aktualne na wszystkich maszynach. Ostatnim etapem wdrożenia jest utworzenie polityk dotyczących przeprowadzania regularnego skanowania całej zawartości dysku twardego oraz pamięci na każdym z komputerów. Dzięki temu będziemy mieli pewność, że nie istnieją nieznane nam zagrożenia, oraz ulepszy to proces raportowania o operatywności hostów. Jeśli powyższe postulaty zostały zrealizowane, to jeszcze nie można stwierdzić ani mieć pewności, że nasze systemy i hosty są bezpieczne. W każdej minucie na świecie powstaje nowe złośliwe oprogramowanie. Niektóre z tych programów potrafią się mutować lub powstają całkiem nowe formy. Jeśli chcemy ustrzec hosty przed infekcją nowym wirusem, musimy wykrywać problemy, zanim nasz program antywirusowy będzie dysponował nową sygnaturą nowego wirusa, ponieważ taka sygnatura może jeszcze nie istnieć i antywirus może nie być w stanie usunąć zagrożenia.

Skutecznym sposobem realizacji takich działań prewencyjnych jest zastosowanie narzędzia Nagios [5]. Nagios jest doskonały do monitorowania sieci, urządzeń sieciowych oraz aplikacji i serwerów. Zapewnia on stałą kontrolę. Dzięki narzędziu Nagios możemy o wiele wcześniej stwierdzić np., że usługi na jakimś serwerze zostały zatrzymane. W ten sposób możemy wnioskować, że na danym komputerze występują problemy związane z jego prawidłową pracą. Nagios wykorzystuje się często do monitorowania krytycznych usług oraz systemów. Oferuje on potężne możliwości oraz umożliwia monitorowanie bardzo wielu istotnych usług i procesów wykonywanych na hostach. W przypadkach wymagających reakcji administratora hosta lub egzystującego na nim serwisu na niezwyczajne zdarzenia lub symptomy zagrożeń bezpieczeństwa bądź ataków staramy się zebrać próbki zawirusowanych

plików i wysyłamy je do producenta oprogramowania antywirusowego. Później oczekujemy już tylko na wydanie nowych sygnatur i modyfikacji ich baz na hostach korporacji. Rysunek 2 przedstawia fotografię ekranu komputera z funkcjonującym narzędziem Nagios, który pokazuje przykład awarii serwera pełniącego funkcję serwera kopii zapasowej.



Rys. 2. Przykład awarii hosta pełniącego funkcję serwera kopii zapasowej wykrytej przez narzędzie Nagios
Fig. 2. Example of failure of the hostacting as a backup server detected by the Nagios tool
Źródło: opracowanie własne.

3. Podsumowanie i wnioski

Ciągle powstają coraz lepsze i bardziej niezawodne narzędzia, dzięki którym poziom bezpieczeństwa hostów oraz infrastruktury IT i systemów produkcyjnych wzrasta. Jest pewne, że należy koncentrować się na walce z tworzonym przez hakerów złośliwym oprogramowaniem oraz na przeciwdziałaniu działalności hakerów łamiących zabezpieczenia w celu wykonywania działań nielegalnych i szkodliwych dla firmy lub korporacji. Coraz

większego znaczenia nabierają zabezpieczenia komputerowych systemów produkcyjnych i komputerowych sieci przemysłowych. Przedstawione tu studium przypadku utrzymywania bezpieczeństwa i zabezpieczenia antywirusowego dotyczy korporacji, której działalność i infrastruktura w dużym stopniu obejmują systemy przemysłowe i wytwórcze. Okazuje się w praktyce, że ochrona antywirusowa i narzędzia typu Nagios w dużym stopniu mogą takie infrastruktury i platformy korporacyjne chronić.

Bibliografia

1. Kocis K., MSCE, Administracja Microsoft Active Directory. Wydawnictwo Helion, Gliwice 2001.
2. AutoIt, http://www.autoitscript.com/site/ (wejście 01.06.2014).
3. Gartner, Gartner Magic Quadrant for Endpoint Protection Platforms, http://www.gartner.com/technology/home.jsp (wejście 30.04.2014).
4. Microsoft, Zapora systemu Windows, http://windows.microsoft.com/pl-pl/windows7/products/features/windows-firewall (wejście 01.06.2014).
5. Nagios, http://www.nagios.org/ (wejście 01.06.2014).

Abstract

Security of computer systems and computer manufacturing industrial networks are becoming increasingly important. The case study here maintain security and antivirus protection applies to corporations whose operations and infrastructure largely includes industrial and manufacturing systems. It turns out in practice that the anti-virus protection, and tools like Nagios, can greatly protect this type of infrastructure and enterprise platforms. Based on analyze of Gartner Endpoint Protection, we should choose faster and effective security software for company. Not always the most expensive software is the best, but software where are implemented strong and good algorithm to detect and remove unwanted software from client. Migration process is very easily where administrator know architecture of network and can create special migration script to implement new anti-virus solution.