

# Zabezpieczanie sieci wieloplatformowej

Autor: Marek  
04.02.2010.  
Zmieniony 04.02.2010.

Przewodnik dotyczący zabezpieczenia sieci wieloplatformowej.

## Wstęp

Dzisiejsze sieci są coraz bardziej różnorodne, zawierają różne rodzaje sprzętu i oprogramowania, pozwalają na uruchomienie wielu systemów operacyjnych, które muszą być w stanie komunikować się ze sobą. Coraz mniej mamy sklepów jedynie z systemem Windows (lub UNIX), natomiast wiele firm posiada domeny systemu Windows równoległe z serwerami UNIX, do których dostęp mają komputery klienckie z systemami Windows, Linux i Mac. Do tej mieszanki należy dodać wiele inteligentnych smartfonów (Windows Mobile, iPhone, Android, Symbian i inne), dla których należy pobrać mail i prawdopodobnie dostać się do innych zasobów sieciowych, a Ty masz prawdziwe wyzwanie. Artykuł ten zajmie się tematem znalezienia odpowiedniej strategii dla zabezpieczenia takiej wieloplatformowej sieci.

## Wyzwania dotyczące zabezpieczenia wieloplatformowej sieci

Trudnym zadaniem może okazać się uruchomienie różnych systemów operacyjnych w taki sposób, aby współpracowały ze sobą. Z tego powodu przy wieloplatformowej sieci uwaga przesuwa się z tematu zabezpieczeń w kierunku pytania jak sprawić, by wszystko dobrze działało. Celem staje się umożliwienie współpracy między platformami, a o ograniczeniach tego współużytkowania można zapomnieć lub przynajmniej ich nie akcentować.

Większość personelu IT jest szkolona w zakresie określonego rodzaju systemu (Windows, UNIX, Mainframe lub inne). Często kadra zarządzająca nie rozumie technologii i zakłada, że jeżeli dana osoba „zna się na komputerach”, to zna się na wszystkich rodzajach systemów. Nawet jeżeli osoba posiada wiedzę ogólną na temat tego, jak zarządzać różnymi platformami, to nie znaczy, że rozumie wszystkie aspekty bezpieczeństwa. Bezpieczeństwo jest bardzo wyspecjalizowanym obszarem, dlatego nie wystarczy sam personel IT, który jest w stanie skonfigurować i zarządzać różnymi rodzajami systemów w sieci, trzeba mieć ludzi, którzy są przeszkoleni w zakresie zabezpieczania różnych rodzajów systemów. Obejmuje to zarówno gruntowne podstawy ogólnych pojęć z zakresu bezpieczeństwa IT, jak i szkolenia specjalistyczne pod kątem poszczególnych dostawców. Pozwoli to na wykorzystanie wbudowanych mechanizmów bezpieczeństwa określonego systemu operacyjnego według swoich potrzeb oraz na zwrócenie się w razie potrzeby do firm zewnętrznych oferujących inne rozwiązania.

Kompetencja częściowo opiera się na zachowaniach rutynowych. Jeżeli dana osoba musi pamiętać różne kroki i procedury dla różnych typów urządzeń, zwiększa się ryzyko pomyłki lub błędnej konfiguracji, co sprawia, że sieć jest bardzo podatna na atak. Dlatego najlepszym wyjściem w przypadku sieci heterogenicznej jest zatrudnienie różnych pracowników, specjalizujących się w różnego rodzaju systemach. Niestety, w czasach gospodarki ekonomicznej, gdzie mantrą jest „zrobić jak najwięcej, jak najmniejszym nakładem środków”, wiele firm nie może pozwolić sobie na luksus zatrudniania wielu specjalistów.

## Wykaz sieci

W wielu środowiskach IT, nie było rzeczywistego planu; zamiast tego sieć „tak wyrosła”, jako że nowe potrzeby wymagały zakupu i wdrożenia nowych systemów, a wszystko to działo się w chaotyczny sposób. Pierwszym krokiem do zabezpieczenia sieci jest dokładna znajomość tego, co się ma, a więc sprawdzenie wykazu sprzętu i oprogramowania. Istnieje wiele narzędzi, które mogą być użyte do wykrywania i dokumentowania elementów, tworzących sieć. Kluczem do sukcesu jest wykorzystanie takiego narzędzia, które obsługuje wszystkie systemy operacyjne, istniejące w Twojej sieci.

Platformy, które są najczęściej pomijane (i w ten sposób pozostawione niezabezpieczone lub zabezpieczone za darmo), to

te uruchamiane na laptopach oraz telefonach, które nie są na stałe podłączone do sieci, jak również te działające na komputerach wirtualnych. Komputer A może posiadać system Windows jako podstawowy system operacyjny, ale jeżeli w systemie tym pracuje wirtualna maszyna z systemem Linux, trzeba traktować ten wirtualny system operacyjny jako kolejny komputer w sieci i odpowiednio go zabezpieczyć. Podobnie należy pamiętać, że wielu użytkowników systemów Linux i Mac również posiada system Windows w środowisku wirtualnym, ponieważ potrzebują niektórych aplikacji systemu Windows, których nie są w stanie uruchomić w jakikolwiek inny sposób. Można tak więc posiadać komputery, zwłaszcza w sytuacji tworzenia lub sprawdzania, z różnymi rodzajami systemów operacyjnych typu „multi-boot”.

Szczegółowy wykaz musi obejmować cały sprzęt i całe oprogramowanie, działające w sieci, nawet jeżeli nie znajduje się w sieci cały czas.

#### Aktualizowanie i/lub modernizacja

Natkanę się na to zdanie w powieści, którą niedawno czytałem („The Doomsday Key” – „Klucz Apokalipsy”; James’a Rollinsa): „Nie ma zamku nie do zdobycia”. To było dobre przypomnienie faktu, że niezależnie od platformy, każdy system, który można podłączyć do Internetu, udostępnia kanał, przez który sprytny napastnik może naruszyć się.

Częstym błędem, w oparciu o nieprawdziwe relacje oraz reklamy, jest założenie, że systemy nie-windowsowskie zawsze są „bezpieczne”. Tak nie jest. Na przykład latem zeszłego roku stwierdzono poważną lukę w zabezpieczeniu jądra w większości wersji systemu Linux, co mogło umożliwić całkowite przejście kontroli nad komputerem przez atakującego. Pełny artykuł na ten temat.

I pomimo powszechnego przekonania, że systemy Mac nie są zagrożone, w maju zeszłego roku firma Apple wypuściła łatę, która skierowana była do 67 (tak, sześćdziesięciu siedmiu) luk w zabezpieczeniach w OS X i przeglądarce Safari - i nadal pozostała luka w języku Java. Pełny artykuł na ten temat.

W rzeczywistości, specjalista ds. zabezpieczeń Mac - Dai Zovi (autor podręcznika „The Mac Hacker’s Handbook”) mówi, że gdy hakerzy decydują się poświęcić swój czas i wysiłek, obierając za swój cel OS X – system operacyjny staje się bardziej segmentem mainstream – i okazuje się, że jest tak samo podatny na atak jak Windows. A współautor - Charlie Miller - twierdzi, że Mac będzie łatwiejszy do wykorzystania. Pełny artykuł na ten temat.

Nie chodzi tu o to, aby ostro krytykować systemy inne niż Windows, ale aby wyprowadzić z błędu personel IT, któremu wydaje się, że tylko komputery z systemem Windows muszą być regularnie aktualizowane. Tak samo ważną jest wprowadzanie aktualizacji dla komputerów z systemem UNIX/Linux oraz Mac, gdy są one wypuszczane na rynek.

Innym ważnym czynnikiem do rozważenia jest to, że w większości przypadków nowe wersje systemu operacyjnego są bardziej bezpieczne niż stare wersje ze wszystkimi łatami. Na przykład, Windows 7 i Windows Vista zawierają szereg mechanizmów zabezpieczeń, takich jak UAC, tryb chroniony IE, szyfrowanie dysków funkcją BitLocker, itd., natomiast XP tego nie ma. Najnowsza wersja OS X - Snow Leopard, w odróżnieniu od swoich poprzedników, posiada wbudowane wykrywanie szkodliwego oprogramowania (choć nie jest ono bardzo zaawansowane). Ponadto posługuje się silniejszymi sumami kontrolnymi w celu ochrony przed atakami typu uszkodzenia pamięci. Najnowsza wersja OpenSUSE wspiera technologię TPM (Trusted Platform Module). W wielu przypadkach, uaktualnienie do najnowszej wersji, niezależnie od używanego systemu operacyjnego, znacznie poprawia bezpieczeństwo.

To samo dotyczy systemów operacyjnych telefonów komórkowych. Na przykład, nowe iPhone’y mają lepsze funkcje zabezpieczeń, takie jak obsługa skomplikowanych haseł, wykorzystujących znaki alfa, znaki numeryczne i symbole czy możliwość zdalnego usuwania danych, czego początkowo iPhone nie miał.

## Uwaga:

Telefony iPhone nadal sprawiają kłopoty z bezpieczeństwem dla środowisk korporacyjnych, ponieważ firma wdraża tylko małą część dostępnych polityk zabezpieczeń programu Exchange, a iTunes, który jest zainstalowany na wszystkich iPhone'ach, może tak samo stanowić zagrożenie bezpieczeństwa.

## Dbanie o podstawy

Takie same podstawowe zasady bezpieczeństwa mają zastosowanie zarówno dla sieci heterogenicznych, jak i homogenicznych, więc jest rzeczą oczywistą, że niezależnie od platform(y), należy:

- Zabezpieczyć się dobrym firewall'em/bramą TMG (threat management gateway) oraz systemami wykrywania w³amañ czy zabezpieczania przed nimi.
- U¿ywaæ oprogramowania antywirusowego i programów typu anti-malware (w tym dla systemów innych ni¿ Windows) oraz aktualizowaæ definicje.
- Wdro¿yæ audyt/monitoring bezpieczeñstwa w celu wykrywania prób naruszenia.
- Wzmocniæ systemy poprzez wy³czenie niepotrzebnych us³ug.
- Zamknæ nieu¿ywane porty.
- Ograniczyæ fizyczny dostêp do systemów.
- Ograniczyæ dostêp administracyjny i dostêp do katalogu g³ównego do osób, które naprawdê tego potrzebuj±; w systemach UNIX ograniczyæ dostêp do katalogu g³ównego do bezpiecznych terminali.
- Wdro¿yæ uprawnienia na poziomie plików; w systemach UNIX zrobiæ partycjê systemu plików i u¿ywaæ partycji &bdquo;tylko do odczytu&rdquo; dla przechowywania plików, które nie zmieniaj± siê czêsto, natomiast list kontroli dostêpu ACL (Access Control Lists) do kompleksowego zarz±dzania uprawnieniami.
- W systemach UNIX ograniczyæ dostêp, jaki maj± procesy do systemu plików, przy u¿yciu polecenia &bdquo;chroot&rdquo; oraz interfejsów &bdquo;unlimit&rdquo;.
- Egzekwowaæ polityki mocnych hase³.
- Wymagaæ dwuetapowego uwierzytelniania w ¶rodowiskach wysokiego bezpieczeñstwa.
- W systemach UNIX korzystaæ z protoko³u SSH (Secure Shell) do zdalnego dostêpu do wiersza poleceñ.
- Korzystaæ z szyfrowania: aby chroniæ pliki na dysku, aby chroniæ dane przechodz±ce przez sieæ, aby chroniæ system operacyjny przed nieautoryzowanym dostêpem.
- Wdro¿yæ infrastrukturê klucza publicznego do wydawania certyfikatów cyfrowych.

## Zatrudnienie niezale¿nego audytora bezpieczeñstwa

Niezale¿ny audyt bezpieczeñstwa mo¿e byæ przydatny do oceny i doradztwa w zakresie wdra¿ania zabezpieczeñ w ka¿dej z³o¿onej sieci, ale w przypadku sieci heterogenicznej jest tym istotniejszy. Firma, która profesjonalnie zajmuje siê audytami bezpieczeñstwa posiada pracowników do¶wiadczonych w zakresie przegl±du ró¿nych typów systemów i jest na bie¿±co w temacie luk oraz nowych rozwi±zañ, z którymi Twoi pracownicy IT mogli siê nie spotkaæ z powodu braku czasu. W czasie audytu mo¿na wykonaæ testy penetracyjne dla rzeczywistej oceny lokalizacji s³abych punktów, mo¿na równie¿ uzyskaæ poradê na temat najskuteczniejszych i najbardziej op³acalnych sposobów na uzupe³nienie braków.

## Podsumowanie

Sieci wieloplatformowe to szczególne wyzwanie w zakresie bezpieczeństwa, którym administratorzy IT muszą stawić czoła, ponieważ sieci takie stają się coraz bardziej popularne. Najważniejszą rzeczą do zapamiętania jest to, że bezpieczeństwo jest procesem, a nie produktem. Należy zastosować takie same podstawowe pojęcia, bez względu na platformę, z tą różnicą, że ich przeprowadzenie odbędzie się w inny sposób w zależności od systemów operacyjnych. Jeśli rozmiar działu IT na to pozwala, w celu zwiększenia ogólnego bezpieczeństwa sieci, należy dokonać podziału kompetencji, który umożliwi, aby różne osoby skupiły się na jednym systemie i w nim się specjalizowały. Jeżeli jest to niemożliwe, warto postarać się o „zewnętrzne oczy” (jeden parę lub jeszcze lepiej kilka), mogące pomóc zidentyfikować luki w zabezpieczeniach, które są zbyt blisko, aby sam byś w stanie je dostrzec, a dodatkowo dostaniesz nowe pomysły na to, jak sobie z nimi poradzić.

Źródło: [www.windowsecurity.com](http://www.windowsecurity.com)