ZARZĄDZENIE Nr 31/2010
Rektora Uniwersytetu Wrocławskiego
z dnia 21 kwietnia 2010 r.

w sprawie wprowadzenia procedury stosowania oprogramowania antywirusowego oraz zapory sieciowej w Uniwersytecie Wrocławskim

Na podstawie art. 66 ust. 2 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. Nr 164, poz. 1365, z późniejszymi zmianami) zarządza się, co następuje:

§ 1. Wprowadza się procedurę stosowania oprogramowania antywirusowego oraz zapory sieciowej w Uniwersytecie Wrocławskim, stanowiącą Załącznik do niniejszego zarządzenia.

§ 2. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Kanclerzowi.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

prof. dr hab. Marek Bojarski

R E K T O R

(Dział Organizacyjny – 2010)

Załącznik
do zarządzenia Nr 31/2010
z dnia 21 kwietnia 2010 r.

Procedura stosowania oprogramowania antywirusowego oraz zapory sieciowej w Uniwersytecie Wrocławskim

§ 1

Wymagania stawiane oprogramowaniu antywirusowemu oraz zaporze sieciowej

1. Każda stacja robocza i serwer podłączony do Uczelnianej Sieci Komputerowej musi posiadać aktualne oprogramowanie antywirusowe oraz zaporę sieciową.
2. Oprogramowanie antywirusowe oraz zapora sieciowa muszą posiadać automatyczną aktualizację z sieci Internet lub z lokalnego repozytorium.
3. Oprogramowanie antywirusowe powinno wykrywać poza wirusami jak największą liczbę złośliwych programów innego rodzaju (np. konie trojańskie, backdoory, exploity, niebezpieczne aplety Javy i ActiveX, spam, itp.). Ponadto powinno się charakteryzować dobrymi narzędziami do analizy heurystycznej, skanowaniem na żądanie całości systemu, bądź jego elementów, skanowaniem w czasie rzeczywistym i niskim obciążeniem systemu.
4. Oprogramowanie antywirusowe powinno posiadać funkcję automatycznego powiadamiania administratora o wystąpieniu incydentu (np. pojawieniu się wirusa w poczcie, próby włamania do systemu, itp.), a także powinno monitorować system on-line i reagować na bieżąco na wszelkie incydenty wg ustawionych przez administratora reguł.
5. Oprogramowanie antywirusowe powinno automatycznie sprawdzać wszelkie podłączane do systemu urządzenia.
6. Oprogramowanie antywirusowe oraz zapora sieciowa powinny być w języku polskim.

§ 2

Zadania kierownika jednostki organizacyjnej

1. Kierownik jednostki organizacyjnej wyznacza administratora sieci lokalnej, który jest odpowiedzialny za wdrożenie i przestrzeganie niniejszej procedury.
2. Kierownik jednostki organizacyjnej ma obowiązek przeznaczyć odpowiednie środki finansowe na zakup w/w oprogramowania.
3. Kierownik jednostki, po otrzymaniu zgłoszenia o wystąpieniu incydentu od administratora sieci lokalnej i po zapoznaniu się ze sprawą, w wyniku której doszło do utraty (kradzieży) danych lub innego rodzaju przestępstwa, zobowiązany jest podjąć właściwe działania dla danej sytuacji, w szczególności zawiadomić właściwe organy Państwa.

§ 3

Zadania administratorów sieci lokalnej

1. Administrator odpowiada za aktualizację oprogramowania i jego baz.
2. Administrator odpowiada za właściwą konfigurację oprogramowania antywirusowego oraz zapory sieciowej. Podczas konfiguracji zapory sieciowej administrator zobowiązany jest zablokować wszystkie porty w zaporze sieciowej zezwalając tylko na komunikację aplikacji niezbędnych do pracy na danej stacji roboczej.

3. Administrator ma obowiązek przeglądania i zabezpieczenia elektronicznie logów oprogramowania antywirusowego oraz zapory sieciowej.
4. Administrator ma obowiązek przeszkolić użytkowników swojej sieci w zakresie użytkowania oprogramowania antywirusowego. Szkolenie powinno zakończyć się pisemnym potwierdzeniem przez szkoloną osobę, że zapoznała się z procedurą i jest świadoma możliwych zagrożeń.
5. Administrator ma obowiązek niezwłocznego reagowania na wszelkie powiadomienia o wystąpieniu incydentu, związanego z zainstalowanym oprogramowaniem antywirusowym i zaporą sieciową.
6. Administrator ma prawo wyłączyć użytkownikom mechanizm przeglądania i wysyłania treści wiadomości w formacie HTML w przeglądarce poczty. W przeglądarkach internetowych ma prawo ograniczyć możliwości otwierania się różnego rodzaju skryptów.
7. Administrator jest zobowiązany do sporządzania zestawu programów freeware akceptowalnych w sieci przez niego zarządzanej.
8. Administrator ma obowiązek odnotowywania w elektronicznym dzienniku wszelkich incydentów, w wyniku których doszło do utraty/kradzieży danych lub innego przestępstwa, a także niezwłocznego zgłaszania tego faktu kierownikowi jednostki organizacyjnej. Ponadto administrator ma obowiązek zabezpieczyć logi dla celów dowodowych.

§ 4

Zadania użytkowników

1. Użytkownicy odpowiadają za poufność swoich danych dostępowych (login i hasło) oraz za dane wytwarzane przez siebie w ramach obowiązków pracy.
2. Użytkownicy nie mogą instalować żadnego oprogramowania bez wiedzy i pisemnej zgody administratora ich lokalnej sieci komputerowej. Przez pisemną zgodę uważa się akceptację przez administratora, pisma z wymienionym oprogramowaniem.
3. Użytkownicy nie mają prawa podłączać do sieci lokalnej uczelni żadnych urządzeń (np. routery, access pointy, switche, notebooki, palmtopy, kamery, aparaty fotograficzne, dyktafony cyfrowe, telefony komórkowe, pendrive, itp.), za wyjątkiem urządzeń służbowych, bez wiedzy i pisemnej zgody administratora ich sieci lokalnej. Przez pisemną zgodę uważa się akceptację, przez administratora, pisma z wymienionym sprzętem.
4. Użytkownicy nie powinni otwierać poczty, załączników poczty oraz plików nieznanego pochodzenia. Dotyczy to również plików pobranych ze stron WWW (np. aplikacji flash, muzyki, krótkiego filmiku, itp.).
5. Użytkownik ma obowiązek pracować na koncie z uprawnieniami użytkownika lub użytkownika zaawansowanego. W wyjątkowych sytuacjach, za wiedzą i pisemną zgodą administratora sieci, może korzystać z konta administratora systemu.
6. Każdy użytkownik powinien zostać przeszkolony w zakresie obsługi oprogramowania antywirusowego oraz zapory sieciowej, a także sposobów powiadamiania administratora sieci lokalnej o wystąpieniu incydentów (np. wirusów) wykrytych przez oprogramowanie antywirusowe. Użytkownicy nieprzeszkoleni mogą żądać przeprowadzenia stosownego szkolenia w ustalonym z administratorem terminie.
7. Po włożeniu zewnętrznego nośnika danych, jeśli nie zostanie on sprawdzony automatycznie przez oprogramowanie antywirusowe lub inne oprogramowanie chroniące, użytkownik ma obowiązek sprawdzenia go ręcznie przy pomocy w/w oprogramowania.

8. W przypadku, gdy oprogramowanie powiadomi użytkownika o wystąpieniu incydentu (np. pojawieniu się wirusa, próbie włamania do systemu, itp.), użytkownik ma obowiązek postępować zgodnie z ustaleniami jakie uzyskał od administratora sieci lokalnej podczas szkolenia.