

## Has³a w systemie Windows: bezpieczeñstwo (cz.3)

Autor: Marek  
17.09.2009.  
Zmieniony 05.05.2010.

Jak sprawiæ, aby has³o w systemie Windows by³o wystarczaj±co mocne do rozwi±zania problemów poruszonych w dwóch poprzednich czê¶ciach tej serii artyku³ów.

### Wstêp

W pierwszych dwóch czê¶ciach tej serii artyku³ów ukaza³em rzeczywisto¶æ polityki hase³ w systemie Windows oraz sposób, w jaki jest ona kontrolowana w ¶rodowisku us³ugi Active Directory. Omówi³em miejsca, gdzie mo¿na znale¼æ politykê hase³ i ustawienia z ni± zwi±zane, które s± przechowywane dla us³ugi Active Directory. Je¶li sobie przypominasz, domy¶lnie znajduj± siê one w Default Domain Policy. Przegl±dn±³em tak¿e technologie, wykorzystywane do ¶amania hase³ Windowsa i opisa³em ograniczenia ka¿dego z ataków. Teraz chcê omówiæ sposób, w jaki mo¿na sprawiæ, ¿e has³o w systemie Windows bêdzie bardziej bezpieczne, co rozwi±¿e wszystkie problemy, które zosta³y poruszone w dwóch pierwszych czê¶ciach tej serii. Omówiê równie¿ mo¿liwo¶ci, zwi±zane z domy¶ln± instalacj± us³ugi Active Directory w systemach Windows 2000/2003/2008, jak równie¿ inne technologie, które s± dostêpne, a s³u¿± do zwiêkszenia ogólnego bezpieczeñstwa has³a.

Po kolei: u¿ywaj frazy

Od prawie trzech lat rozpowszechniam w¶ród osób prywatnych oraz organizacji wiedzê, ¿e je¶li popatrzy siê na has³o z innej perspektywy, to ±atwiej je zapamiêtaæ, ±atwiej wystukaæ na klawiaturze i w ten sposób w du¿o ±atwiejszy sposób mo¿na uzyskaæ d³u¿sze has³o. Typowe has³o, które u¿ytkownik mo¿e wykorzystaæ to:

Am3r1c@

Powy¿sze has³o spe³nia wymagania dotycz±ce z³o¿ono¶ci, ale jest trudne do zapamiêtania i na pewno nie jest ±atwe do wystukania na klawiaturze. Dlatego te¿ u¿ytkownicy zapisz± sobie to has³o na karteczce i przyklej± na monitorze albo po³o¿± pod klawiatur±, itp. Zamiast czego¶ tak archaicznego jak to has³o, nale¿y u¿yæ has³a ... hmm, to znacz±y czego¶ na kszta³t has³a-frazy, np.:

Jestem MVP polityki grupowej.

Lub

Pojecha³em do Niemiec w czasie ostatnich wakacji.

Uwaga:

Przeczytaj ka¿de z trzech powy¿szych hase³ i hase³-fraz, a nastêpnie spróbuj szybko wystukaæ ka¿de z nich na klawiaturze. Zobaczysz, ¿e has³a-frazy s± znacznie ±atwiejsze do napisania, a nawet zapamiêtania!

Ponieważ wszystkie hasła-frazy pokonują LM, ataki słownikowe i Tablice Tęczowe, możesz teraz pozwolić swoim użytkownikom na utrzymywanie jednego hasła przez dłuższy czas, nawet cały rok!

W ostatnim artykule z tej serii, omówię jak powinna wyglądać dobra polityka haseł, w jaki sposób zapewnić jej wdrożenie, jak zapewnić, aby była ona taka sama na każdym komputerze (w tym na lokalnym Menedżerze Zabezpieczeń Kont SAM) oraz jakie inne technologie (hasła szczegółowe oraz polityki haseł &bdquo;specops&rdquo;) mogą być wykorzystane, aby otrzymać i wdrożyć dobre hasła.

Zapewnienie zgodności polityki haseł dla kont domeny oraz lokalnych użytkowników

Wbudowana konfiguracja usługi Active Directory zapewnia, że wszystkie konta użytkowników (te przechowywane w usłudze Active Directory i te zapisane na lokalnym SAM na każdej stacji roboczej i serwerze) mają tę samą politykę haseł. Jednakże, można to zmienić poprzez powiązanie i skonfigurowanie GPO na poziomie jednostki organizacyjnej (OU), gdzie jednostka organizacyjna przechowuje konta komputera. W takim przypadku stacje robocze i serwery (ale nie kontrolery domeny) mogą mieć lokalny SAM kont użytkowników należący do innej polityki haseł niż SAM kont użytkowników domeny.

W celu utrzymania spójnej polityki haseł dla wszystkich użytkowników, można &bdquo;narzucić&rdquo; je obiektowi GPO, który gromadzi ustawienia polityki haseł dla kont użytkowników domeny. I znowu, domyślnie jest to Default Domain Policy. Aby to zrobić, kliknij prawym przyciskiem myszy na obiekt GPO, a następnie wybierz opcję &bdquo;Enforce Menu&rdquo;. Rysunek 1 pokazuje, jak to wygląda po konfiguracji.

Rysunek 1: Narzucenie Domyślnej Polityki Domeny zapewni, że wszyscy użytkownicy kont lokalnych SAM będą używać tej samej polityki haseł

Mechanizm wielu polityk haseł dla domeny wykorzystujący technologię Microsoft Multiple Password Policies per Domain

Microsoft, aby sprostać współczesnym wymogom, daje możliwość posiadania wielu polityk haseł w jednej domenie Active Directory. Nie jest super nowością, ale z pewnością dołącza istotne udoskonalenie. Technologia ta jest dostępna tylko w domenie Windows Server 2008, gdzie na wszystkich kontrolerach domeny działa system Windows Server 2008. Również na domenie musi być uruchomiony funkcjonalny poziom systemu Windows Server 2008. Technologia ta jest określana jako szczegółowa polityka haseł.

W takim przypadku można skonfigurować wiele polityk haseł. Oznacza to, że możesz mieć następujące rzeczy:

- Użytkownicy IT muszą używać haseł składających się z 25 znaków
- Użytkownicy HR muszą używać haseł składających się z 20 znaków

- Wszyscy pozostali użytkownicy muszą używać haseł składających się z 17 znaków.

Są to strony tego rozwiązania jest fakt, że nie jest ono skonfigurowane w Polityce Grupowej. Zamiast tego trzeba stworzyć dodatkowe obiekty usługi Active Directory pod Kontenerem Ustawień Haseł. Aby przeglądać i konfigurować te nowe obiekty, można użyć przystawki ADSIEDIT.MSC, pokazanego na rysunku 2.

Rysunek 2: ADSIEDIT.MSC może zostać użyty do stworzenia dodatkowych szczegółowych polityk haseł w domenach Windows Server 2008

Aby utworzyć dodatkowe obiekty, musisz kliknąć prawym przyciskiem myszy na Kontener Ustawień Haseł, a następnie wybrać „New”, a potem „Object”. Kreator prowadzi użytkownika przez to, co musi zostać skonfigurowane.

Przenoszenie polityk haseł na następny poziom

Przez lata firma Microsoft dawała nam możliwość kontroli za pomocą polityki haseł, a teraz tej kontroli mamy nawet więcej, dzięki szczegółowym politykom haseł w systemie Windows Server 2008. Jednak, jeśli chcesz przenieść ustawienia polityki haseł w domenę systemu Windows na poziom, który daje maksymalną kontrolę nad hasłami, musisz pobrać narzędzie takie jak Password Policy ze Special Operations Software. Narzędzie to działa głównie w usłudze Active Directory oraz jest dopasowane do Polityki Grupowej w taki sposób, jakby działały szczegółowe polityki haseł!

Przy pomocy tego narzędzia możesz dokonać następujących konfiguracji:

- ustawić dowolną kombinację ograniczeń dotyczących hasła: małe litery, duże litery, cyfry i znaki specjalne
- ustawić dla każdej polityki różne zasady wygasania hasła, powszechnie nazywane wiekiem hasła
- umożliwić ustalanie następujących po sobie znaków w haśle
- umożliwić ustanawianie haseł pierwotnych
- automatycznie wysłać maila o wygaśnięciu hasła
- ustalić dodatkowe wymogi polityki haseł: wyrażenia powszechne; uniemożliwienie stosowania słów pisanych wspak; uniemożliwienie stosowania cyfr jako ostatniego znaku.

Rysunek 3 ilustruje jak wygląda interfejs dla Polityki Haseł.

Rysunek 3: Specops Password Policy jest szczegółowym narzędziem polityki haseł dla domen w systemie Windows

#### Podsumowanie

Hasła w systemie Windows zawsze są narażone na ataki. Istnieje wiele narzędzi jak i powodów, dla których atakujący mógłby starać się zdobyć hasła w systemie Windows. Wiele z tych ataków jest aktualnych i dość łatwych. Tak więc, należy chronić własne hasła i hasła użytkowników w sieci, którymi się zarządza. Ustawienia domyślne w środowisku Windows powinny zostać zmienione, w szczególności te, dotyczące uwierzytelniania LanManager. Należy zalecić użytkownikom, aby nie zapisywali ani nie przesyłali swoich haseł, gdyż jest to zbyt łatwe do odkrycia. Kluczem jest tu edukacja na temat tworzenia dobrego, mocnego, skomplikowanego, długiego hasła ..., a raczej hasła-frazy! Wykorzystanie narzędzia, które dostarcza wielu haseł w tej samej domenie, a nawet narzuca bardziej skomplikowane i restrykcyjne hasła, może sprawić, że ochrona będzie lepsza, a hasła bardziej bezpieczne. Jeśli domyślne polityki haseł są przechowywane na miejscu, a atakujący dostanie się do hasła lub SAMa, istnieje duże ryzyko utraty ochrony! Lepiej chroń i zabezpieczaj swoje hasła już od dzisiaj!

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