Akademia Handlowa Nauk Stosowanych w Radomiu

Bezpieczeństwo systemów komputerowych Laboratorium 2

Radom 2021/2022

1. Cel zadania

Współczesne systemy Windows przeszły długą drogę rozwoju. Od czasu rozwoju jądra NT firma Microsoft zmieniła wcześniejsze priorytety względem tworzenia funkcjonalności systemu, stawiając przede wszystkim na stabilność i bezpieczeństwo. Celem zadania będzie przeanalizowanie najnowszych elementów zabezpieczeń systemu i sprawdzenie ich skuteczności.

2. Potrzebne narzędzia.

- kompletny zestaw komputerowy z systemem operacyjnym Windows i Windows Server, odpowiednio w wersjach co najmniej 10 i 2019
LUB
- kompletny zestaw komputerowy z dowolnym system operacyjnym
- oprogramowanie do wirtualizacji (VMWare, Hyper-B, VirtualBox, kvm)
- systemy Windows jak wykazano wcześniej

3. Informacje wstępne

Społeczeństwo przyzwyczaiło się do przekonania, że systemy z rodziny Windows nie dają odpowiedniej gwarancji bezpieczeństwa. Twierdzenia te są oparte o przeświadczeniu, że niemal codziennie możemy przeczytać o kolejnych wirusach, robakach czy trojanach czy złośliwym oprogramowaniu szyfrującym, które pojawiają się na rynku właśnie na system Windows. Jednak trzeba sobie uświadomić, że system ten jest najczęściej wybieranym systemem na komputery osobiste i laptopy, przez co większość złośliwego oprogramowania powstaje właśnie na systemy z rodziny Windows. Pomimo tego coraz mniej tego typu oprogramowania może wyrządzić realne szkody końcowemu użytkownikowi. Wpływ na ten stan ma zarówno rozwój aplikacji do spraw zabezpieczeń, jak i narzędzia oraz usługi dostarczane wraz z Windows. W samym systemie, co najmniej w jego podstawowych elementach (jądro, folder z plikami systemowymi, obraz przywracania), trudno teraz znaleźć możliwość przeprowadzenia nieautoryzowanej operacji przy braku odpowiednich uprawnień (niekiedy wręcz operacje są niemożliwe do wykonania jeżeli nie jesteśmy użytkownikiem SYSTEM lub WindowsInstaller).
Oczywiście nawet najlepsze zabezpieczenia nie będą w stanie ochronić naszego oprogramowania, jeżeli administrator należycie go nie zabezpieczy oraz nie skonfiguruje usług odpowiadających za bezpieczeństwo. Chociaż system, w przeciwieństwie do swoich wersji jeszcze sprzed 8-10 lat wprowadza coraz więcej zabezpieczeń już podczas instalacji, wiele z tych rozwiązań, w domyślnej opcji, będzie działało wadliwie bądź wcale.

Najważniejszymi zmianami, jakich dokonano na przestrzeni lat, a które skutkują zwiększeniem bezpieczeństwa systemowego, to:

- Domyślne wyłączenie konta administratora
- Domyślne wyłączenie i zblokowanie włączania użytkownika Gość (Guest)
- Domyślnie działające UAC (User Account Control)
- Dostępne logowanie w systemie konta zewnętrznego (chociaż to może mieć zarówno wydźwięki pozytywne jak i negatywne)
- System logowania Hello, pozwalający lepiej zabezpieczyć dostęp do naszego komputera
- Możliwość zaszyfrowania całego magazynu danych już na poziomie systemu
- Możliwość wykonywania administracji porzez serwer OpneSSH
- Domyślne wykorzystanie PowerShell zamiast linii CMD (bezpieczniejszego, acz bardziej zawodnego systemu zarządzania CLI).

4. Przebieg.

Laboratorium ma charakter doświadczalno-praktyczny i ma na celu ukazanie podstawowych możliwości narzędzi i konfiguracji systemu Windows:

- Wykorzystanie wolumenów logicznych dla systemu Windows – możliwości instalacji i konfiguracji
- Szyfrowanie przestrzeni magazynowej zarówno za pomocą BitLocker jak i np. VeraCrypt; sprawdzenie skuteczności dostępu do danych (np. Szybkości ładowania się systemu przed i po zaszyfrowaniu, sprawdzenie czy jest cokolwiek widoczne, gdy dysk zostanie podpięty do innego systemu itp.)
- Wykorzystanie Windows Hello celem logowania się za pomocą przygotowanego USB (zamiast hasła)
- Sprawdzenie możliwości wykonania w systemie Windows narzędzia sudo (formalnie nie istnieje). W tym wypadku można wypróbować polecenie runas w CMD lub parametr runas w PowerShell LUB zaproponować inną aplikację/rozwiązanie
- Jednym z lepszych rozwiązań ochrony systemów i komputerów przed ewentualnym złośliwym oprogramowaniem jest system wirtualizacji systemów komputerowych. Jednak maszyny wirtualne są przeważnie postrzegane jako wolniejsze, do tego ograniczają możliwości oprogramowania (np. Słaby dostęp do kart graficznych). System Windows oferuje możliwość uruchamiania obrazów VHD(x) bezpośrednio z BCD. Czy tego typu rozwiązanie faktycznie może przyczynić się do zabezpieczenia komputera? Czy możliwe jest “mrożenie” systemu w określonym stanie (np. konfiguracji oprogramowania) celem szybkiego przywrócenia jej funkcjonalności w przypadku uszkodzenia systemu operacyjnego? Jak można takiej konfiguracji dokonać?
- Jak zabezpieczyć połączenia zdalne w systemie Windows? Jakie są trzy możliwe sposoby zarządzania zdalnego systemem Windows? Które z nich jest najbezpieczniejsze?

5. Zakończenie

Rozwiązanie należy przesłać w postaci PDF (NIE MUSI MIEĆ FORMY SPRAWOZDANIA!) zrzuty ekranowe dokumentujące działanie określonej funkcjonalności i/lub krótki opis wskazanej funkcjonalności (nawet w postaci listowej jakie przynosi korzyści dla bezpieczeństwa) na adres piotr_dobosz@int.pl, w temacie wiadomości zawierając frazę [AHNS_BSK].

6. Dodatki

https://support.microsoft.com/en-us/account-billing/set-up-a-security-key-as-your-verification-method-2911cacd-efa5-4593-ae22-e09ae14c6698
https://support.microsoft.com/en-us/windows/sign-in-to-your-microsoft-account-with-windows-hello-or-a-security-key-800a8c01-6b61-49f5-0660-c2159bea4d84
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/boot-to-vhd--native-boot--add-a-virtual-hard-disk-to-the-boot-menu?view=windows-11
https://www.urtech.ca/2022/03/solved-what-is-the-difference-between-a-snapshot-and-a-backup/