AVET
Information and Network Security

Ochrona systemów Windows XP po wygaśnięciu wsparcia

AVET INS Infrastructure Security Practice

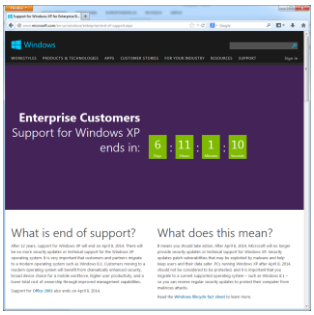
Wprowadzenie

8 kwietnia 2014 roku Microsoft kończy wsparcie dla Windows XP. Niniejszy dokument zawiera istotne z perspektywy bezpieczeństwa zalecenia, których celem jest utrzymanie wymaganego poziomu bezpieczeństwa po wygaśnięciu wsparcia. Dokument powstał głównie na potrzeby rozwiązań bankomatowych, ale może być stosowany także do systemów XP używanych w innych zastosowaniach.

Zgodnie z informacją od Microsoft, wsparcie dla systemu Windows XP zostanie zakończone dnia 8 kwietnia 2014.

Więcej informacji:
http://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx

Ogólne wytyczne



1. Należy zainstalować wszystkie wydane poprawki (hotfix) bezpieczeństwa.
2. Systemy XP należy umieścić za systemem zaporowym, który zapewnia kompletną inspekcję ruchu sieciowego (proxy).
3. W systemach XP należy zainstalować aktualne rozwiązanie chroniące przed szkodliwym oprogramowaniem, które nadal wspiera tą platformę.
4. W systemach XP należy zainstalować Service Pack 3 (jeśli nie zostało to jeszcze zrobione) – SP3 wprowadza istotne zmiany w zabezpieczeniach systemów XP oraz wymagany jest przez inne komponenty.
5. Należy wdrożyć system SIEM i monitorować logi z systemu operacyjnego oraz ruch sieciowy do i z systemu.
6. Jeśli oprogramowanie korzysta z przeglądarki, rozważ instalację innej niż Internet Explorer, która nadal wspiera platformę Windows XP i dostarcza do niej aktualizację.

Dodatkowe wytyczne techniczne

1. Należy deaktywować zbędne i niebezpieczne usługi poprzez ich całkowite wyłącznie (ustawienie manualny start nie jest wyłączeniem).
2. Należy ograniczyć uprawnienia serwisów, które są uruchomione (po wykonaniu kroku 1).
3. Należy ograniczyć liczbę kont w systemie.
4. Należy nadać silne hasła do kont, które zostały (min 8 znaków).
5. Należy ograniczyć uprawnienia uruchamianych aplikacji.
6. Aplikacje uruchamiane w kontekście konta bankomatu nie mogą mieć prawa modyfikacji rejestru, plików systemowych oraz katalogów z plikami (exe, dll, itp.) z których korzysta aplikacja.
7. Należy wyłączyć zdalny dostęp do rejestru.
8. Należy ograniczyć prawa do zapisu do rejestru.
9. Należy włączyć audyt zdarzeń a w szczególności audyt zdarzeń z kategorii bezpieczeństwo. Audytować należy wszystkie zdarzenia w tej kategorii czyli nie tylko działania które zakończyły się niepowodzeniem, ale także te które zakończyły się sukcesem.
10. Należy usunąć polecenie runas.exe.
11. Należy wyłączyć mechanizm NULL Session.
12. Należy wyłączyć zdalny dostęp do stacji dysków i CD/DVD.

Pytania / Pomoc

Jeśli masz pytania odnośnie powyższych zaleceń lub masz problem z ich implementacją w praktyce skontaktuj się z nami: avet@avet.com.pl.

O AVET INS

Od 1997 AVET Information and Network Security dostarcza usługi konsultingowe do największych organizacji sektora finansowego oraz IT w Europie. Nasze usługi oferujemy w Polsce, Holandii, Słowacji, Wielkiej Brytanii, Rumunii i Ukrainie.