Wprowadzenie podstawowych zasad zabezpieczeń na stacji roboczej z systemem Windows 10 w urzędzie jednostki samorządu terytorialnego (JST)

**Uwaga: prezentowany materiał przeznaczony jest dla osób posiadających przynajmniej minimalną wiedzę z zakresu administrowania systemem Windows 10.**

# Dlaczego należy wprowadzić proponowane zasady zabezpieczeń?

Bezpieczeństwo stacji roboczej, zwanej też urządzeniem użytkownika końcowego (End User Device - EUD), jest równie ważne jak stosowanie zabezpieczeń na granicy sieci lokalnej i sieci rozległej. Jak pokazują statystyki, w związku z upowszechnieniem się ataków na systemy informatyczne z użyciem phishingu[[1]](#footnote-1), to właśnie działanie użytkownika końcowego staje się poważnym zagrożeniem dla zasobów informacyjnych urzędu. Wprowadzenie proponowanych zabezpieczeń w istotny sposób ogranicza możliwość prowadzenia ataku z zainfekowanej stacji roboczej na pozostałe komponenty systemu informatycznego urzędu.

# Jakie minimalne zasady zabezpieczeń należy wdrożyć na EUD?

Opis minimalnych zasad zabezpieczeń EUD znajduje się w pliku „Zasady zabezpieczeń poziomu 0.doc” (w załączonych materiałach pod artykułem)

# Czy można wdrożyć minimalne zasady zabezpieczeń z poziomu sterownika domeny?

Najlepszym mechanizmem wdrożenia zasad zabezpieczeń jest użycie mechanizmu sterownika domeny do wymuszania zabezpieczeń grupowych z wykorzystaniem obiektu zasad grupy (Group Policy Object - GPO). W takim przypadku, przy każdym logowaniu do domeny wymuszane będą aktualne zasady zabezpieczeń, nawet wtedy, gdy na EUD zmieniono je na takie, które nie są akceptowane w urzędzie.

# Co zrobić, gdy z jakiegoś powodu nie można wymusić zasad zabezpieczeń z poziomu sterownika domeny?

Jeżeli z jakiegoś powodu nie można wymusić zasad zabezpieczeń z poziomu sterownika domeny, zasady zabezpieczeń należy wdrożyć lokalnie. Można tego dokonać na dwa sposoby:

* użyć wbudowanego Menadżera Zabezpieczeń w systemie Windows 10,
* użyć programu LGPO.exe.

W każdym z tych sposobów wymagane są uprawnienia administratora na EUD.

Menadżer Zabezpieczeń znajduje się w zakładce „Narzędzia administracyjne systemu” i nosi nazwę „Zasady zabezpieczeń lokalnych”. Narzędzie to nie jest rekomendowane do wprowadzania zmian dużej liczby zasad zabezpieczeń na dużej liczbie komputerów. Łatwo w taki przypadku popełnić błąd.

Lepszym rozwiązaniem jest zastosowanie programu LGPO.exe

# Jak wprowadzić zabezpieczenia stacji roboczej z systemem operacyjnym według zaleceń za pomocą narzędzia LGPO.

Przedstawiana instrukcja pozwala na zastosowanie przygotowanych zestawów zasad zabezpieczeń GPO Microsoft SecCon0 na lokalnym komputerze. Należy pamiętać, że na komputerach niedodanych do domeny, ustawienia będą trwale obowiązujące (do kolejnej zmiany). Na komputerach w domenie, część (lub wszystkie) z ustawień może zostać nadpisana przez ustawienia GPO z poziomu domeny, lokacji lub jednostek organizacyjnych.

1. Pobieramy LGPO z witryny Security Compliance Toolkit <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
2. Klikamy na Download 
3. Z listy plików wybieramy LGPO.zip



1. Wypakowujemy plik LGPO.zip. Dostajemy dwa pliki: LGPO.exe – właściwe narzędzie i plik LGPO.pdf – instrukcję.



1. Wypakowujemy zawartość archiwum SecConL1.zip (z politykami GPO Microsoft SecConL1). Po wypakowaniu archiwum, dostajemy strukturę folderów, gdzie każdy folder odpowiada ustawieniom jednego z poziomów SecCon. W SecConL1/SecConL1/Policies znajdują się interesujące nas obiekty GPO.

*Uwaga: Zestaw zasad zabezpieczeń SecConL1 zawiera zasady zabezpieczeń, które z uwagi na ograniczenia sprzętowe (np. brak modułu TPM), nie zostaną zaimplementowane w danym EUD. Brak możliwości instalacji niektórych zasad zabezpieczeń z wyżej opisanych powodów nie spowoduje błędnej instalacji pozostałych. Taki poziom zasad zabezpieczeń bywa określany jako SecConL0.*



1. Uruchamiamy cmd jako administrator (Menu start -> cmd -> uruchom jako Administrator/lub CTRL+Shift+Enter)
2. Przechodzimy do folderu z wypakowanym LGPO.exe



1. Uruchamiamy ldp.exe aby zastosować nasze obiekty GPO dla lokalnego komputera (local GPO). Składnia: LGPO.exe /g *<Ścieżka do polityk SecCon (katalog Policies)>*

Np: LGPO.exe /g c:\Seccon\SecCon\SecConL1\SecConL1\Policies

**Uwaga:** przed uruchomieniem LGPO /g, zalecamy wykonanie kopii zapasowej aktualnych zasad zabezpieczeń za pomocą polecenia LGPO.exe /b <ścieżka do katalogu backupu>.



1. Wykonujemy restart komputera.
2. Polityki zostały zastosowane.

# Ważne podsumowanie

Zanim dokonasz zmian na wszystkich stacjach roboczych w urzędzie sprawdź na jednej z nich wpływ tych zmian na stosowane aplikacje. Pamiętaj, że niektóre stacje robocze posiadają oddzielne zasady zabezpieczeń wynikające z polityki bezpieczeństwa systemów, z którymi współpracują (np. aplikacja ŹRÓŁO). Zmian nie wykonujemy na stacjach roboczych wykorzystywanych do przetwarzania informacji niejawnych, dla których zasady zabezpieczeń ustalane są przez ABW.

1. Phishing - metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji [↑](#footnote-ref-1)