PORADNIK PWCYBER

Zasada minimalnych uprawnień na stacjach roboczych

Autor: Securivy sp. z o.o. — członek klastra Cyber Made in Poland



Klaster Cyber Made in Poland, NIP 6762583919 / KRS 0000854192 (dalej Partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przygotowanych przez firmę Securivy sp. z o.o. (NIP 7792534607 / KRS 0000944866), będącą członkiem klastra, w ramach Programu PWCyber (zwanych dalej „Materiałami"), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych. Partner oświadcza, że materiały nie naruszają praw osób trzecich.

Spis treści

Streszczenie 3
1. Problem: stałe prawa administratora jako norma, nie wyjątek 3
   Kto najczęściej potrzebuje uprawnień lokalnego administratora 3
2. Dlaczego lokalny administrator to realne ryzyko 4
3. Zasada minimalnych uprawnień i jej umocowanie normatywne 5
4. Endpoint Privilege Management jako mechanizm realizacji 6
5. Jak bezpiecznie odebrać prawa administratora — plan wdrożenia 7
   Etap 1. Inwentaryzacja i pomiar stanu wyjściowego 7
   Etap 2. Zdefiniowanie polityk i wyjątków 8
   Etap 3. Wdrożenie pilotażowe 8
   Etap 4. Odebranie uprawnień i przejście na model standardowy 8
   Etap 5. Utrzymanie i optymalizacja 8
6. Just-in-Time: koniec z uprawnieniami „na stałe" 9
7. Typowe błędy wdrożeniowe 9
8. Dobre praktyki — lista kontrolna 9
9. Podsumowanie 10

Spis rysunków

Rysunek 1. Porównanie przebiegu ataku na dwóch stacjach 5
Rysunek 2. Schemat przepływu podniesienia uprawnień na żądanie 7
Rysunek 3. Mapa drogowa wdrożenia w pięciu etapach 8

Streszczenie

Nadmiarowe uprawnienia lokalnego administratora na stacjach roboczych to jeden z najczęściej niedocenianych i zarazem najgroźniejszych czynników ryzyka w organizacji. Konto z prawami administratora znacząco poszerza powierzchnię ataku, ułatwia instalację złośliwego oprogramowania, ruch boczny w sieci i eskalację uprawnień. Jednocześnie odebranie tych praw bywa odkładane, ponieważ postrzega się je jako źródło uciążliwości dla użytkowników i obciążenia dla działu IT.

Ten poradnik pokazuje, dlaczego zasada minimalnych uprawnień (*ang. Principle of Least Privilege* - PoLP) jest fundamentem higieny bezpieczeństwa punktów końcowych, jak umocowana jest w wymaganiach normatywnych oraz — przede wszystkim — jak wdrożyć ją w praktyce bez paraliżowania pracy użytkowników. Opisujemy model zarządzania uprawnieniami na punktach końcowych (*ang. Endpoint Privilege Management - EPM/PEDM*) oraz mechanizm nadawania uprawnień „na żądanie" i „na czas" (*ang. Just-in-Time - JIT*).

1. Problem: stałe prawa administratora jako norma, nie wyjątek

W wielu organizacjach użytkownicy pracują na co dzień z uprawnieniami lokalnego administratora. Przyczyny są zwykle historyczne i pragmatyczne: część aplikacji wymaga podniesionych uprawnień do instalacji lub aktualizacji, użytkownicy techniczni potrzebują ich do własnej pracy, a dział IT — chcąc unikać ciągłych zgłoszeń — nadaje je „na zapas".

Skutkiem jest sytuacja, w której prawa administratora, z założenia wyjątkowe, stają się stanem domyślnym. Każda taka stacja to nie tylko ryzyko dla samego urządzenia, ale węzeł, przez który zagrożenie może rozprzestrzenić się na całą sieć.

Kto najczęściej potrzebuje uprawnień lokalnego administratora

Prawa administratora trafiają najczęściej do ról technicznych, które rzeczywiście potrzebują ich w codziennej pracy. Zrozumienie, kto i do czego ich używa, jest punktem wyjścia do zaprojektowania modelu, który nie zablokuje tym rolom pracy.

- **Programiści i deweloperzy** — instalacja bibliotek, pakietów, kompilatorów i środowisk uruchomieniowych, konteneryzacja, uruchamianie lokalnych serwerów i baz danych, debugowanie oraz instalacja sterowników. To rola generująca najwięcej uzasadnionych żądań podniesienia uprawnień.

- **Zespół IT i administratorzy** — instalacja i konfiguracja oprogramowania, zarządzanie usługami systemowymi, sterownikami i ustawieniami stacji roboczych.
- **Help-Desk i wsparcie techniczne** — diagnostyka, instalacja poprawek i aktualizacji, konfiguracja aplikacji bezpośrednio na stacjach użytkowników.

Właśnie dla tych ról model zarządzania uprawnieniami na punktach końcowych (EPM) oraz nadawania uprawnień na czas (JIT) ma największą wartość. Pozwala im wykonać potrzebne czynności bez utrzymywania stałych praw administratora, zachowując pełną rozliczalność. Odebranie uprawnień nie oznacza więc odebrania możliwości pracy — zmienia jedynie sposób, w jaki uprawnienia są przyznawane.

2. Dlaczego lokalny administrator to realne ryzyko

Konto administratora lokalnego zmienia jakościowo przebieg potencjalnego incydentu. Poniższe mechanizmy nie są teoretyczne — odpowiadają typowym etapom rzeczywistych ataków.

Instalacja i uruchomienie złośliwego oprogramowania. Większość mechanizmów obronnych systemu operacyjnego oraz wiele technik ransomware zakłada, że kod działa w kontekście uprawnień użytkownika. Uprawnienia administratora pozwalają wyłączyć zabezpieczenia, zmodyfikować rejestr, zainstalować sterowniki czy usługi i utrwalić obecność w systemie.

Eskalacja i ruch boczny. Przejęcie stacji z prawami administratora daje napastnikowi punkt wyjścia do pozyskania poświadczeń (np. z pamięci procesów), a następnie do przemieszczania się między systemami w sieci. Ograniczenie uprawnień lokalnych istotnie utrudnia ten etap.

Ryzyko niezłośliwe. Nie każdy incydent wynika ze świadomego ataku. Użytkownik z prawami administratora może przypadkowo zainstalować niepożądane oprogramowanie, zmienić krytyczną konfigurację lub wyłączyć mechanizm ochronny. Minimalizacja uprawnień redukuje również ten rodzaj ryzyka.

Zacieranie rozliczalności. Współdzielone lub powszechne konta administracyjne utrudniają jednoznaczne przypisanie działań do osób, co osłabia zarówno prewencję, jak i analizę powłamaniową.



Rysunek 1. Porównanie przebiegu ataku na dwóch stacjach

Opis alternatywny (WCAG 2): Dwie równoległe ścieżki ataku. Górna, na stacji z prawami lokalnego administratora: zainfekowanie, podniesienie uprawnień, wyłączenie zabezpieczeń, instalacja złośliwego oprogramowania, ruch boczny, szyfrowanie danych. Dolna, na stacji z ograniczonymi uprawnieniami: zainfekowanie, próba podniesienia uprawnień zablokowana, atak zatrzymany.

3. Zasada minimalnych uprawnień i jej umocowanie normatywne

Zasada minimalnych uprawnień mówi, że każdy użytkownik, proces i usługa powinny dysponować wyłącznie tymi uprawnieniami, które są niezbędne do wykonania konkretnego zadania — nie większymi i nie na dłużej, niż to konieczne.

Zasada ta nie jest jedynie dobrą praktyką, lecz znajduje odzwierciedlenie w wymaganiach normatywnych i regulacyjnych, między innymi:

- **Norma PN-EN ISO/IEC 27001** — w obszarze kontroli dostępu i zarządzania uprawnieniami uprzywilejowanymi (kontrole z grupy dotyczącej zarządzania dostępem).
- **Dyrektywa NIS2** — nakładająca na podmioty kluczowe i ważne obowiązek stosowania środków zarządzania ryzykiem, w tym higieny cyberbezpieczeństwa i kontroli dostępu (art. 21).
- **Krajowy system cyberbezpieczeństwa** — w zakresie środków technicznych i organizacyjnych adekwatnych do ryzyka.
- **Wytyczne ramowe** (np. CIS Controls, NIST) — wprost wskazujące ograniczenie uprawnień administracyjnych jako jedną z podstawowych i najskuteczniejszych zabezpieczeń.

Wspólny mianownik tych wymagań jest jasny: uprawnienia uprzywilejowane mają być kontrolowane, ograniczone i rozliczalne.

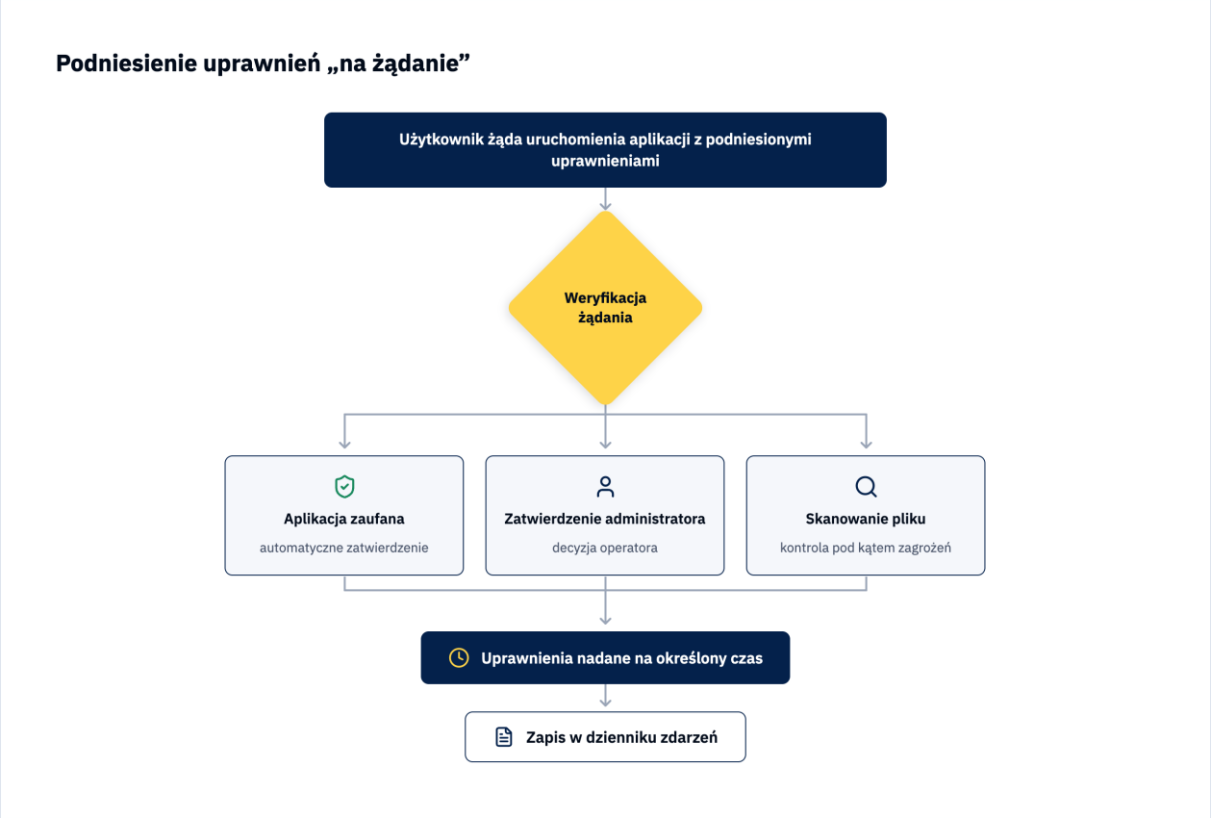
4. Endpoint Privilege Management jako mechanizm realizacji

Bezpośrednie odebranie użytkownikom praw administratora bez zapewnienia mechanizmu obsługi uzasadnionych potrzeb kończy się zwykle falą zgłoszeń i presją na przywrócenie uprawnień. Rozwiązaniem tego dylematu jest klasa narzędzi określana jako **zarządzanie uprawnieniami na punktach końcowych** (*ang. Endpoint Privilege Management - EPM*; w części źródeł *PEDM — Privilege Elevation and Delegation Management*).

Idea polega na tym, że użytkownik pracuje na co dzień jako konto standardowe, a podniesienie uprawnień następuje **punktowo**: dla konkretnej aplikacji lub czynności, na określony czas, w kontrolowany i rejestrowany sposób. Kluczowe cechy tego podejścia:

- **Podniesienie na poziomie aplikacji, nie sesji.** Zamiast nadawać użytkownikowi pełne prawa administratora, uprawnienia otrzymuje pojedyncza aplikacja lub czynność. Reszta środowiska pozostaje w kontekście standardowym.
- **Przepływ zatwierdzania** (*ang. approval workflow*)**.** Żądanie podniesienia uprawnień może być zatwierdzane automatycznie (dla zaufanych, wcześniej zaakceptowanych aplikacji) lub kierowane do administratora.
- **Nadawanie na czas** (Just-in-Time). Uprawnienia obowiązują tylko przez zdefiniowany okres, po którym wygasają. Eliminuje to problem uprawnień „stałych" i nieużywanych.
- **Rejestrowanie i rozliczalność.** Każde podniesienie uprawnień jest zapisywane — kto, kiedy, do czego i na jakiej podstawie. To materiał zarówno do audytu, jak i do analizy incydentów.
- **Kontrola oprogramowania.** Możliwość zdefiniowania list aplikacji dozwolonych i zablokowanych oraz — w części rozwiązań — skanowania plików pod kątem zagrożeń przed podniesieniem uprawnień.

Dojrzałe rozwiązania z tej klasy, dostępne również na rynku polskim, realizują model pracy na koncie standardowym z możliwością podniesienia uprawnień na poziomie aplikacji, z przepływem zatwierdzania, nadawaniem na czas i pełnym rejestrowaniem żądań. Obsługują zwykle stacje robocze i serwery w środowiskach Windows, macOS oraz Linux. Wybór konkretnego narzędzia powinien wynikać z analizy potrzeb organizacji — zakresu obsługiwanych systemów, modelu zatwierdzania, integracji z posiadaną infrastrukturą oraz sposobu rejestrowania i raportowania.



Rysunek 2. Schemat przepływu podniesienia uprawnień na żądanie

Opis alternatywny (WCAG 2): Diagram przepływu. Użytkownik zgłasza żądanie uruchomienia aplikacji z podniesionymi uprawnieniami. System ocenia żądanie w trzech możliwych ścieżkach: automatyczne zatwierdzenie dla aplikacji zaufanej, zatwierdzenie przez administratora, lub skanowanie pliku pod kątem zagrożeń. Po pozytywnej ocenie uprawnienia są nadawane na określony czas i zapisywane w dzienniku zdarzeń.

5. Jak bezpiecznie odebrać prawa administratora — plan wdrożenia

Odebranie uprawnień to projekt, nie jednorazowe przełączenie ustawienia. Poniżej proponowany, etapowy przebieg, który minimalizuje ryzyko oporu użytkowników i przestojów.

Etap 1. Inwentaryzacja i pomiar stanu wyjściowego

Ustal, którzy użytkownicy i które stacje dysponują dziś prawami administratora oraz do czego faktycznie ich używają. Bez tej wiedzy trudno przewidzieć skutki odebrania uprawnień. Dobrą praktyką jest okres obserwacji, w którym narzędzie EPM działa w trybie audytu — rejestruje żądania podniesienia uprawnień, nie zmieniając jeszcze uprawnień użytkowników.

Etap 2. Zdefiniowanie polityk i wyjątków

Na podstawie danych z inwentaryzacji zdefiniuj:

- listę aplikacji, które można podnosić automatycznie (zaufane, powszechnie używane);
- czynności wymagające zatwierdzenia przez administratora;
- aplikacje zablokowane;
- ścieżkę awaryjną (tzw. *break-glass*) na wypadek braku dostępu do zatwierdzającego.

Etap 3. Wdrożenie pilotażowe

Rozpocznij od reprezentatywnej grupy pilotażowej — obejmującej zarówno użytkowników nietechnicznych, jak i wymagających (np. programistów, administratorów). Pilotaż weryfikuje realistyczność polityk i pozwala skorygować je przed szerokim wdrożeniem.

Etap 4. Odebranie uprawnień i przejście na model standardowy

Po walidacji polityk odbierz prawa administratora użytkownikom, przełączając ich na konta standardowe z obsługą podniesień „na żądanie". Kluczowa jest tu komunikacja: użytkownik musi wiedzieć, że nie traci możliwości pracy, lecz zmienia się sposób uzyskiwania uprawnień.

Etap 5. Utrzymanie i optymalizacja

Monitoruj wzorce żądań, aktualizuj listy aplikacji, przeglądaj wyjątki i redukuj liczbę żądań wymagających ręcznego zatwierdzenia. Celem jest stan, w którym większość uzasadnionych potrzeb obsługiwana jest automatycznie, a interwencja administratora dotyczy tylko sytuacji nietypowych.



Rysunek 3. Mapa drogowa wdrożenia w pięciu etapach

Opis alternatywny (WCAG 2): Oś czasu z pięcioma etapami: 1. inwentaryzacja i audyt, 2. definiowanie polityk i wyjątków, 3. pilotaż, 4. odebranie uprawnień i przejście na konta standardowe, 5. utrzymanie i optymalizacja.

6. Just-in-Time: koniec z uprawnieniami „na stałe"

Model nadawania uprawnień na czas (Just-in-Time) jest logicznym rozszerzeniem zasady minimalnych uprawnień w wymiarze czasowym. Zamiast pytania „kto powinien mieć uprawnienia administratora", zadaje się pytanie „kto potrzebuje ich teraz i na jak długo".

W praktyce oznacza to, że uprawnienia:

- są nadawane w odpowiedzi na konkretną potrzebę;
- obowiązują przez zdefiniowany, krótki czas;
- wygasają automatycznie, bez konieczności ręcznego odbierania.

Efektem jest radykalne ograniczenie tzw. stałej ekspozycji — liczby kont, które w dowolnym momencie mogłyby zostać wykorzystane do ataku. To jedno z najskuteczniejszych pojedynczych działań ograniczających skutki przejęcia poświadczeń.

7. Typowe błędy wdrożeniowe

Odebranie uprawnień bez mechanizmu obsługi potrzeb. Najczęstszy błąd. Prowadzi do fali zgłoszeń, frustracji i presji na wycofanie zmiany. EPM/JIT ma być wdrożony przed odebraniem uprawnień, nie po.

Zbyt restrykcyjne polityki na starcie. Brak listy zaufanych aplikacji powoduje, że każda czynność wymaga zatwierdzenia — obciąża to IT i zniechęca użytkowników. Politykę należy kalibrować na podstawie danych z fazy audytu.

Pominięcie ścieżki awaryjnej. Brak mechanizmu *break-glass* może w sytuacji krytycznej zablokować pracę. Ścieżka awaryjna musi istnieć, ale być rejestrowana i objęta przeglądem.

Brak komunikacji z użytkownikami. Zmiana bez wyjaśnienia jest odbierana jako utrudnienie. Z wyjaśnieniem — jako element bezpieczeństwa, w którym użytkownik uczestniczy.

Traktowanie serwerów jak stacji roboczych. Środowiska serwerowe rządzą się inną logiką i wymagają odrębnych polityk. Nie należy przenosić na nie wprost reguł ze stacji roboczych.

8. Dobre praktyki — lista kontrolna

- Praca na koncie standardowym jest stanem domyślnym; prawa administratora są wyjątkiem, nie normą.

- Podniesienie uprawnień następuje na poziomie aplikacji lub czynności, nie całej sesji.
- Każde podniesienie ma określony czas obowiązywania i wygasa automatycznie.
- Zaufane aplikacje obsługiwane są automatycznie; czynności wrażliwe wymagają zatwierdzenia.
- Wszystkie żądania i podniesienia są rejestrowane i okresowo przeglądane.
- Istnieje udokumentowana, rejestrowana ścieżka awaryjna.
- Polityki dla stacji roboczych i serwerów są rozdzielone.
- Wdrożenie poprzedza faza audytu, a odebranie uprawnień — pilotaż.

9. Podsumowanie

Ograniczenie uprawnień lokalnego administratora to jedno z działań o najlepszym stosunku efektu do kosztu w całym obszarze bezpieczeństwa punktów końcowych. Zmniejsza powierzchnię ataku, utrudnia rozprzestrzenianie się zagrożeń i wprost odpowiada na wymagania normatywne — od ISO/IEC 27001, przez NIS2, po krajowe regulacje.

Warunkiem powodzenia jest jednak podejście procesowe: odebranie uprawnień musi być poprzedzone wdrożeniem mechanizmu obsługi uzasadnionych potrzeb (EPM) i uzupełnione o model nadawania uprawnień na czas (JIT). Tak przeprowadzona zmiana nie obniża produktywności — przeciwnie, porządkuje sposób korzystania z uprawnień i czyni go rozliczalnym.