**SELinux**

SELinux(Security-Enhanced Linux) jest mechanizmem kontroli dostępu w systemach opartych na jądrze Linux, który dodaje dodatkowe warstwy zabezpieczeń. Jego główną funkcją jest zwiększenie poziomu bezpieczeństwa poprzez narzucenie polityk bezpieczeństwa na działanie programów i użytkowników w systemie. Został zaprojektowany aby zwiększyć bezpieczeństwo systemu poprzez kontrole dostępu dla procesów, plików, portów sieciowych i innych zasobów. SELinux może zostać skonfigurowany tak, aby uwzględniał różne konteksty bezpieczeństwa dla różnych użytkowników, co pozwala na kontrole dostępu do zasobów systemu w zależności od uprawnień poszczególnych użytkowników.

W przeciwieństwie do SharePoint, SELinux nie zapewnia narzędzi do udostępniania plików ani pracy w zespole w takim sensie, w jakim to robi platforma SharePoint.

Mechanizm SELinux składa się z trzech głównych elementów[5]:

* Jądro z interfejsami LSM – SELinux wykorzystuje interfejsy LSM(Linux Security Modules), co umożliwia realizację kontroli dostępu do różnych obiektów w systemie Linux. Dzięki interfejsom SELinux ma możliwość wprowadzania własnej polityki bezpieczeństwa, zdefiniowanej w Policy, co daje bardziej precyzyjne zarządzanie uprawnieniami i kontrola dostępu.
* Modyfikacje wybranych programów – Instalacja SELinuxa może wymusić pewne zmiany w niektórych programach systemowych (jak np. ssh, ls, ps, login), nawet jeśli pierwotnie te zmiany nie miały na celu poprawiania bezpieczeństwa. Jest to związane z integracją SELinuxa z danymi programami i zapewnieniem poprawnego oraz bezpiecznego ich funkcjonowania. Rola administratora w tym przypadku polega na implementacji tych zmian w trakcie instalacji SELinuxa.
* Polityka bezpieczeństwa(Policy) – SELinux dostarcza z systemem Linux funkcjonalną i domyślnie skonfigurowaną politykę bezpieczeństwa. Ta polityka jest konfigurowalna i umożliwia administratorowi dostosowanie zasad bezpieczeństwa do potrzeb konkretnej instalacji. Administrator musi zapoznać się ze składnią konfiguracji polityki, aby dostosować ją do wymagań swojego środowiska. W Policy znajdują się reguły, które mówią jakie działania są zezwolone dla użytkownika oraz do jakich obiektów ma dostęp.