RZECZPOSPOLITA POLSKA
PROKURATURA KRAJOWA
DEPARTAMENT
DO SPRAW CYBERPRZESTĘPCZOŚCI
I INFORMATYZACJI
ul. Postępu 3
02-676 WARSZAWA

Warszawa, dnia – data zgodna z podpisem

1001-12.0481.26.2026

Pani/Pan
Prokurator Regionalny
Prokurator Okręgowy
/wszyscy/

Szanowni Państwo Prokuratorzy,

W związku z prowadzonym procesem wymiany lub aktualizacji systemów kadrowo-płacowych w jednostkach organizacyjnych prokuratury szczebla regionalnego oraz okręgowego, zwracam się z prośbą o stosowanie wskazanych poniżej wymagań wdrożeniowych oraz określanie ich w zawieranych umowach wdrożeniowych.

Architektura nowego lub zaktualizowanego systemu kadrowo-płacowego musi spełniać najlepsze praktyki cyberbezpieczeństwa, a co za tym idzie reprezentować wymagany poziom odporności cyfrowej na ataki, wycieki danych lub nieuprawnione dostępy do danych przez osoby nie będące uprawnionymi pracownikami poszczególnych jednostek. W celu zapewnienia jednolitego, porównywalnego i bezpiecznego wdrożenia w skali całej organizacji, wszystkie jednostki zobowiązane są uruchamiać systemy kadrowo-płacowe oraz finansowo-księgowe z uwzględnieniem poniższych wymagań.

1. Zabrania się bezpośredniego dostępu, bez nadzoru, do systemów kadrowo-płacowych przez firmy trzecie. Dostęp serwisowy powinien odbywać się pod nadzorem pracownika prokuratury.

2. Zabrania się przekazywania firmom trzecim zrzutów baz danych, kopii produkcyjnych, eksportów, raportów, logów lub innych informacji zawierających dane przetwarzane w systemach kadrowo-płacowych, w szczególności danych wrażliwych, danych osobowych oraz danych archiwalnych. Jakiekolwiek przekazanie danych poza środowisko OPDR (w tym na potrzeby analizy błędów) dopuszczalne jest wyłącznie w postaci danych zanonimizowanych lub zmaskowanych, po uprzednim uzgodnieniu z Zamawiającym i w niezbędnym zakresie.
3. Zabrania się wykorzystania lokalnych kont serwisowych dla administratorów, dostawców lub kont systemowych. Wszelkie konta serwisowe muszą zostać utworzone w centralnym Active Directory prokuratura.gov.pl. Pracownicy firm zewnętrznych muszą posiadać konta imienne utworzone zgodnie z zasadą najniższych niezbędnych uprawnień. Wymagane jest rozdzielenia ról i uprawnień administracyjnych (administracja OS / administracja bazy danych / administracja aplikacji), z ograniczeniem uprawnień do poziomu niezbędnego dla realizacji zadań.
4. Dostęp zdalny pracowników wykonawcy na etapie utrzymania może odbywać się tylko w trybie nadzorowanym. Zabrania się jakichkolwiek innych kanałów administracyjnych, w szczególności bezpośrednich połączeń VPN, tuneli, narzędzi zdalnego pulpitu lub kont „awaryjnych" niepowiązanych z tożsamością imienną.
5. Wymagane jest wprowadzenie segmentacji sieci LAN celem zabezpieczenia nieuprawnionego dostępu do systemu kadrowo-płacowego, a dostęp do komponentów systemu musi być utworzony tylko dla uprawnionych pracowników danej jednostki. Wymagane jest, aby komunikacja między komponentami systemu była ograniczona do niezbędnych portów i usług.
6. Wymagane jest, aby baza danych aplikacji została rozdzielona logicznie od serwisu www w ramach dwóch oddzielnych serwerów wirtualnych.
7. Wymagane jest, aby baza danych przechowująca dane systemu kadrowo-płacowego została skonfigurowana jako klaster wysokiej dostępności (active-passive).

8. Wdrażane rozwiązanie należy zintegrować z centralną domeną Active Directory prokuratura.gov.pl. Wymagane jest stosowanie kont imiennych dla użytkowników końcowych, celem utworzenia śladu audytowego systemu.
9. Wymagane jest, aby system kadrowo-płacowy prowadził rejestrowanie zdarzeń (log audytowy) w sposób umożliwiający jednoznaczną identyfikację użytkownika oraz odtworzenie przebiegu działań. Logi muszą być zabezpieczone przed modyfikacją i usunięciem. Wymagana jest możliwość eksportu logów do rozwiązania zewnętrznego (np. SIEM) w formacie tekstowym/ustrukturyzowanym.
10. Wymagane jest, aby bazy danych zostały zainstalowane na oprogramowaniu MS SQL Server na infrastrukturze udostępnianej przez Prokuraturę Krajową w OPDR i jednocześnie nie dopuszcza się zastosowania wersji Express lub innego rozwiązania typu serwer SQL. W celu zapewnienia jednolitego modelu w danym regionie oraz uproszczenia utrzymania, wymaga się uruchamiania środowisk bazodanowych w ramach regionu w spójnym modelu; co do zasady przyjmuje się jeden klaster SQL per region.
11. W celu utrzymania jednolitego środowiska na potrzeby serwera www, rekomenduje się wykorzystanie serwera Apache lub IIS zainstalowanych na systemach operacyjnych Rocky Linux w wersji minimum 9.7 lub Windows Server 2022/2025.
12. W celu ograniczenia widoczności danych w zakresie systemu, wymagany jest granularny podział uprawnień użytkowników wynikający z ich zakresu obowiązków.
13. Wymagane jest posiadanie procedury tworzenia kopii zapasowej systemu kadrowo-płacowego oraz jej regularne wykonywanie zgodnie z ustalonym harmonogramem.
14. Wymagane jest prowadzenie aktualnej dokumentacji odzwierciedlającej faktyczny stan systemu umożliwiającej odtworzenie systemu do stanu obecnego w przypadku awarii.
15. Wymagane jest posiadanie procedury aktualizacji systemu kadrowo-płacowego dostarczonej przez wykonawcę w ramach utrzymania systemu. Aktualizacje

powinny być wykonywane niezwłocznie po oficjalnym udostępnieniu najnowszej wersji przez dostawcę. Zalecane jest przeprowadzenie testów aktualizacji na środowisku nieprodukcyjnym. Regularna aktualizacja środowiska systemu kadrowo-płacowego dotyczy również systemów operacyjnych oraz bazy danych

16. Wymagane jest utrzymanie konwencji nazewniczej zgodnie z wytycznymi dla środowisk Prokuratury Krajowej oraz jednostek podległych.
17. W przypadku konieczności dostępu do danych archiwalnych, wymaga się, aby dane archiwalne były przechowywane na innym dedykowanym zasobie nie połączonym z nową aplikacją.
18. Zaleca się aby system źródłowy podczas wdrożenia nowego rozwiązania został zmigrowany w całości. Nie jest zalecane utrzymywanie poprzedniego systemu w okresie wykraczającym ponad rok od momentu migracji, z uwagi na narastające ryzyka bezpieczeństwa oraz koszty utrzymania..

Z poważaniem

Dyrektor Departamentu do Spraw

Cyberprzestępczości i Informatyzacji

Podpisane przez: Agnieszka Teresa Gryszczyńska
Data: 2026.02.20 14:06:19 CET
Podpis niekwalifikowany