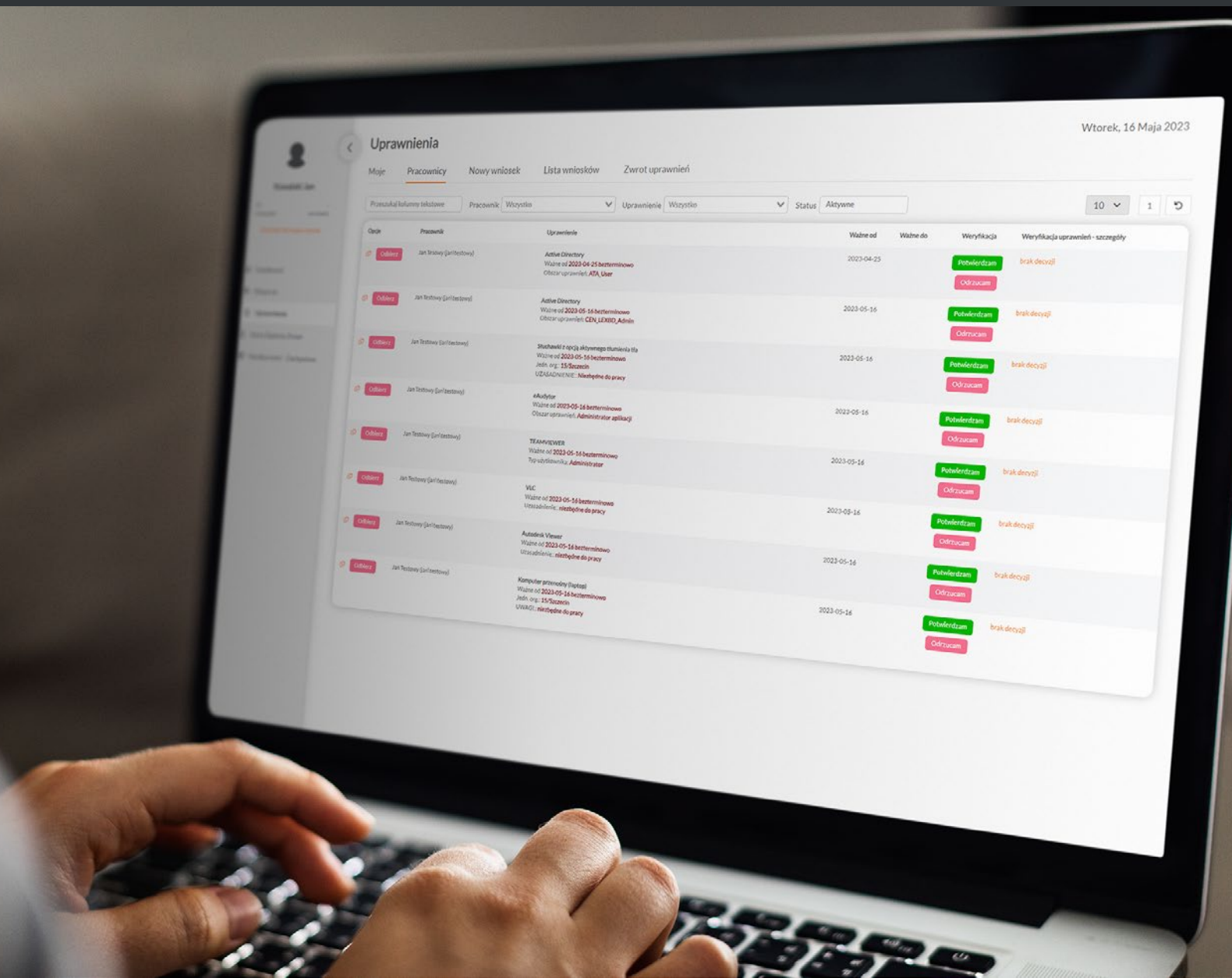
eauditor

SYSTEM ZARZĄDZANIA UPRAWNIENIAMI (IAM)

Kompleksowe oprogramowanie automatyzujące procesy nadawania, weryfikacji oraz odbierania uprawnień do systemów informatycznych.



KORZYŚCI Z WDROŻENIA SYSTEMU

eauditor

BEZPIECZEŃSTWO

Wdrożenie systemu zapewnia możliwość bieżącego monitorowania uprawnień przez przełożonych poprzez zapewnienie im prostego dostępu (za pomocą Panelu Pracownika) do uprawnień posiadanych przez pracowników. Pracownicy również mają dostęp do uprawnień i mogą wnioskować o odebranie im niezasadnie przydzielonych uprawnień. Wzrost bezpieceństwa wynika z przeniesienia nadzoru nad uprawnieniami do niższych poziomów struktury organizacyjnej.

PODGLĄD AKTYWNYCH UPRAWNIEŃ

Kierownicy mogą w każdej chwili sprawdzić posiadane przez ich podwładnych uprawnienia do systemów informatycznych. Dostęp do widoku możliwy jest w Panelu Pracownika. Pracownicy również mogą weryfikować swoje uprawnienia.

AUTOMATYZACJA

System umożliwia przyspieszenie procesów nadawania, odbierania oraz audytu uprawnień do systemów informatycznych. Dzięki temu podmioty zatrudniające kilka tysięcy pracowników mogą znacząco skrócić czas procesowania wnioskowania o uprawnienia. Osoba wnioskująca nie musi wiedzieć, kto odpowiada za rozpatrzenie wniosku. W wyniku zdefiniowania relacji pomiędzy kartotekami system automatycznie wskazuje osobę rozpatrującą. Weryfikacja zgodności uprawnień realizowana jest w dwóch etapach – przez bezpośredniego przełożonego oraz dział IT.

PROSTE WNIOSKOWANIE O UPRAWNIENIA

Osoba wnioskująca nie musi wiedzieć, kto odpowiada za rozpatrzenie wniosku. W wyniku zdefiniowania relacji pomiędzy kartotekami system automatycznie wskazuje osobę rozpatrującą. Weryfikacja zgodności uprawnień realizowana jest w dwóch etapach – przez bezpośredniego przełożonego oraz dział IT. Pozwala to ograniczyć liczbę pracowników z nieprawidłowymi dostępami do systemów informatycznych.

POWIADOMIENIA

Każdy uczestnik procesu zarządzania uprawnieniami otrzymuje automatyczne powiadomienia e-mail dotyczące utworzenia oraz zmiany statusu wniosku o uprawnienia. Nie ma konieczności logowania się do systemu w celu weryfikacji statusu wniosku.

AUDYT

System umożliwia zdefiniowanie cyklicznej weryfikacji nadanych już uprawnień do systemów informatycznych. Proces weryfikacji jest zautomatyzowany i regularnie przypomina o konieczności przeprowadzenia audytu. Dzięki temu osoby decyzyjne mają pewność, że weryfikacja odbędzie się w terminie.

KORZYŚCI Z WDROŻENIA SYSTEMU

eauditor

INTEGRACJA

MS Active Directory/eHelpDesk

Wbudowane w system mechanizmy integracji z usługami i produktami usprawniają pracę administratora systemu. Możliwy jest m.in.: automatyczny import struktury organizacyjnej, import danych pracowników, bezpośrednie przesyłanie zgłoszeń do działów wsparcia technicznego czy bieżący podgląd uprawnień w Panelu Pracownika.

PANEL PRACOWNIKA

Panel Pracownika jest webową aplikacją dostępną dla pracowników z poziomu pulpitu komputera (ikona) bez konieczności logowania. Panel automatycznie identyfikuje zalogowanego użytkownika i uwierzytelnia go z wykorzystaniem SSO.

SYSTEM DOSTOSOWANY DO KAŻDEJ BRANŻY

Siłą systemu jest pełna konfigurowalność na etapie wdrożenia. Możliwe jest samodzielne tworzenie kartotek oraz definicji uprawnień. Może znaleźć zastosowanie w obszarze obsługi wniosków o dostęp do np. maszyn produkcyjnych czy pomieszczeń.

PRZEZNACZENIE

Zadaniem systemu jest uproszczenie i zautomatyzowanie procesu zarządzania uprawnieniami.
System pozwala na realizację procesów:

- wnioskowania o nadanie uprawnień do pojedynczych systemów/aplikacji,
- wnioskowania o nadanie uprawnień do grup uprawnień/profilów,
- wnioskowania o zwrot uprawnień,
- weryfikacji uprawnień formalnych,
- weryfikacji uprawnień faktycznych,
- bieżącego monitorowania uprawnień,
- wykonania audytu uprawnień,
- wnioskowania o zmiany w oprogramowaniu,
- fizycznego i automatycznego nadania uprawnień w innych systemach/usługach.

DLA KOGO?

System przeznaczony jest dla podmiotów posiadających liczną, złożoną i rozproszoną infrastrukturę. Szybkie korzyści z wdrożenia systemu są widoczne w podmiotach posiadających ponad tysiąc pracowników mających dostęp do zasobów informatycznych.

KARTOTEKI

Listy słownikowe niezbędne do redagowania i utworzenia wniosku. Administrator systemu może samodzielnie definiować kartoteki, wprowadzać do nich dane, modyfikować je, tworzyć między nimi dowolne powiązania oraz wprowadzać w obrębie nich komentarze, które zostaną wyświetlane podczas tworzenia wniosku.

DEFINICJE UPRAWNIEŃ

Zdefiniowane kartoteki są wykorzystywane do utworzenia definicji uprawnień do pojedynczych systemów informatycznych oraz profili (grup systemów). Odpowiednio zdefiniowany wniosek będzie kierowany do właściwej grupy wsparcia w systemie eHelpDesk.

SZABLONY ZATWIERDZEŃ

Zdefiniowanie szablonów zatwierdzania umożliwia jednoznaczne określenie osoby lub osób odpowiedzialnych za akceptację lub odrzucenie wniosku. Definiowane są również powiadomienia e-mail, za pomocą, których informujemy wszystkich uczestników procesu o aktualnym etapie i statusie wniosku.

AUDYT BILANSU OTWARCIA

Funkcja służy do weryfikacji aktualnych (bieżących) uprawnień nadanych pracownikom. Po zaimportowaniu danych do systemu administrator może sprawdzić zgodność nadanych dostępów do systemów informatycznych.

NOWY WNIOSEK

Formularz wniosku umożliwiający rejestrację następujących informacji:
osoba wnioskująca, osoba, której dotyczy wniosek, przedmiot wniosku, data ważności uprawnienia.

LISTA WNIOSKÓW

Widok zawierający listę wniosków w podziale na bieżące statusy. Z poziomu listy wniosków możliwe jest dokonanie zmian w obrębie wniosku, zmiany akceptującego, śledzenie historii wniosku oraz wprowadzenie podziału listy według przedmiotu wniosku.

PODGLĄD NADANYCH UPRAWNIEŃ

Kierownik (przełożony) posiada podgląd uprawnień nadanych wszystkim swoim podwładnym. Pracownik posiada podgląd wszystkich swoich uprawnień. Widok bieżących uprawnień pozwala na utworzenie duplikatu wniosku na istniejące już uprawnienie.

ZWROT UPRAWNIEŃ

Osoba decyzyjna może w każdej chwili odebrać wybrane bądź wszystkie uprawnienia pracownikom. Pracownik w obrębie swoich uprawnień może zawnioskować o ich zwrot. Zapobiega to nieautoryzowanym dostępom do programów i zasobów, zwiększając tym samym poziom bezpieczeństwa IT.

WERYFIKACJA UPRAWNIEŃ

W systemie możliwa jest dwuetapowa weryfikacja nadanych uprawnień:

- **weryfikacja formalna** – polega na potwierdzeniu uprawnień przez bezpośredniego przełożonego pracownika. System umożliwia generowanie automatycznych powiadomień o konieczności przeprowadzenia weryfikacji formalnej. Po weryfikacji formalnej możliwe jest rozpoczęcie procesu weryfikacji faktycznej.
- **weryfikacja faktyczna** – przeprowadza ją dział wsparcia technicznego. Polega na sprawdzeniu uprawnień zweryfikowanych już pod kątem formalnym. Dział IT potwierdza lub odrzuca uprawnienia.

PROCES OBSŁUGI WNIOSKU

eauditor

1 NOWY WNIOSEK O UPRAWNIENIE

Osoba wnioskująca po zalogowaniu do systemu lub z poziomu panelu pracownika tworzy nowy wniosek.

2 WYBÓR PRACOWNIKA LUB GRUPY PRACOWNIKÓW, KTÓRYCH DOTYCZY WNIOSEK

Osoba wnioskująca z dostępnej listy wskazuje pracownika lub grupę pracowników, których ma dotyczyć wniosek.

3 WYBÓR PRZEDMIOTU WNIOSKU

Osoba wnioskująca wskazuje, zgodnie z definicją uprawnień, przedmiot wniosku o uprawnienia. W ramach jednego formularza może wnioskować o nadanie wielu uprawnień, nawet jeśli akceptacji dokonują różne osoby weryfikujące.

4 WSKAZANIE OKRESU WAŻNOŚCI UPRAWNIEŃ

Osoba wnioskująca ustala czas ważność uprawnień (czas nieokreślony lub wskazuje konkretny przedział czasu).

5 UZUPEŁNIENIE WYMAGANYCH PARAMETRÓW

Osoba wnioskująca wypełnia wymagane pola we wniosku, które zostały zdefiniowane w szablonach zatwierdzeń.

6 WYSŁANIE WNIOSKU

Osoba wnioskująca wysyła wniosek, który następnie trafia w odpowiedniej kolejności do osób wskazanych w szablonach zatwierdzeń.

7 AKCEPTACJA LUB ODRZUCENIE WNIOSKU

Osoba decyzyjna otrzymuje powiadomienie e-mail oczekujacym na rozpatrzenie wniosku. Po zalogowaniu do systemu lub z poziomu panelu pracownika dokonuje akceptacji lub odrzucenia wniosku.

8 POWIADOMIENIE MAILOWE

Każdy uczestnik procesu jest informowany o zmianie statusu wniosku za pomocą powiadomień e-mail.

9 REALIZACJA WNIOSKU

Informacja o akceptacji wniosku przez właściciela biznesowego przekazywana jest do określonej grupy wsparcia w celu wygenerowania uprawnienia.

10 GENEROWANIE UPRAWNIEŃ

Dział IT nadaje rzeczywiste (fizyczne) uprawnienia do systemów informatycznych. Możliwe jest automatyczne generowanie uprawnień za pomocą skryptów (np. założenia konta w domenie, ustalenie hasła, praw dostępu do folderów współdzielonych, założenie konta e-mail itp.). Lista możliwości generowania uprawnień jest nieograniczona w wyniku użycia silnika PowerShell.

BEZPIECZEŃSTWO

System był oceniany na zgodność z OWASP Application Security Verification Standard (ASVS), wersja 4.0.3 na poziomie 2, wykluczając punkty wymagające analizy kodu źródłowego.

OWASP ASVS określa najlepsze praktyki w zakresie testowania mechanizmów bezpieczeństwa aplikacji i aplikacji internetowych.

MODEL ZAKUPU I LICENCJONOWANIE

System jest oferowany w modelu subskrypcji (12/24/36M) lub licencji wieczystej. Cena systemu jest zależna od liczby administratorów systemu (liczba kont dla osób uprawnionych do administrowania systemem) oraz liczby użytkowników występujących w procesach (w praktyce liczba ta jest równa liczbie osób w MS Active Directory).

INSTALACJA/URUCHOMIENIE/WDROŻENIE

- Proces wdrożenia systemu rozpoczyna się od dokładnej analizy rodzaju i ilości systemów, rodzaju uprawnień oraz metod procesowania wniosków.
- Instalacja i konfiguracja systemu wykonywana jest w infrastrukturze klienta zdalnie.
- Proces wdrożenia składa się z utworzenia kartotek oraz powiązań między nimi i zdefiniowania wszystkich procesów. Kolejny krok obejmuje przeprowadzenie tzw. bilansu otwarcia uprawnień - importowane są dane z obecnych systemów zawierających uprawnienia (o ile takie występują), MS Active Directory oraz tworzone są niezbędne integracje. Proces tworzenia bilansu otwarcia może być tworzony wielokrotnie aż do uzyskania bezbłędnych list uprawnień. Po utworzeniu bilansu otwarcia uprawnień przeprowadzona jest dwuetapowa weryfikacja (weryfikacja formalna i weryfikacja faktyczna).
- Po zakończeniu procesu wdrożenia praca systemu jest monitorowana przez okres 3 miesięcy oraz wprowadzane są niezbędne korekty.

INTEGRACJE

System jest zintegrowany z następującymi usługami/produktami:

- Microsoft Active Directory - w zakresie importu struktury organizacyjnej oraz osób (pracowników), uwierzytelniania logowania,
- CAS – w zakresie uwierzytelniania logowania,
- Panel Pracownika – w zakresie wnioskowania, przeglądu oraz akceptacji uprawnień,
- eHelpDesk – w zakresie procesowania wniosków o uprawnienia.

Zapraszamy do kontaktu

https://www.eauditor.eu/identity-access-management/