Zapewnij standard PCI DSS

8MAN
Access Rights Management.
Only much Smarter.

The Payment Card Industry Data Security Standard (PCI DSS) to zestaw zaleceń zaprojektowanych aby wszystkie firmy procesujące, przechowywujące lub transmitujące informacje zawarte na kartach kredytowych zapewniały bezpieczne środowisko. Standard stosowany jest do wszystkich organizacji i kupców którzy akceptują, transmitują lub przechowują jakiekolwiek dane posiadaczy kart, niezależnie od ilości transakcji.

8MAN to intuicyjne narzędzie służące do zarządzania uprawnieniami, pomagające zbudować odporny proces wspierający wiele wymagań stawianych przed przedsiębiorstwami. Rozwiązanie ogranicza prawa dostępu do niezbędnych podstaw, minimalizując tym samym zagrożenia dla bezpieczeństwa danych. Organizacje używające serwerów plików, Active Directory, Exchange i SharePoint mogą w łatwy sposób zobaczyć, zarządzać, zabezpieczać i delegować prawa dostępu z pomocą **8MAN**.

Poniższa lista zapewnia szybki wgląd w jaki sposób **8MAN** może pomóc spełnić wymagania **PCI DSS** takie jak ograniczenie dostępu do danych posiadacza karty przypisując unikatowy numer do każdej osoby mającej dostęp do komputera, monitorując wszystkie dostępy do zasobów sieciowych i danych posiadacza karty, a także utrzymania polityk dotyczących bezpieczeństwa informacji.

Spełnianie wymagań PCI DSS za pośrednictwem 8MAN pozwala przedsiębiorstwom osiągnąć zarówno zgodność systemów IT jak i najlepsze praktyki w tym zakresie. Aby sprawdzić jak 8MAN może pomóc Twojemu przedsiębiorstwu, skontaktuj się z nami aby umówić się na spotkanie lub demonstrację online.

Wdrożenie standardu PCI DSS

8MAN
Access Rights Management.
Only much Smarter.

Zalecenie		Opis	8MAN
Zalecenie 7: Ograniczenie dostępu do danych posiadacza karty.	7.1 Ograniczyć dostęp do składników systemu i danych posiadacza karty jedynie do pracowników których praca wymaga takiego dostępu. Ograniczenia dostępu muszą zawierać następujące zalecenia:	7.1.1 Ograniczenie prawa dostępu uprzywilejowanych użytkowników do najmniejszych możliwych, niezbędnych do wykonywania pracy.	8MAN Acces Reports sprawdza którzy użytkownicy mają gdzie dostęp. Wszystkie zmiany praw dostępu są zapisywane wraz z informacją wyjaśniającą dlaczego uprawnienia zostały modyfikowane.
		7.1.2 Przydzielanie uprawnień dla użytkowników oparte o indywidualne potrzeby i obowiązki dla poszczególnych stanowisk pracy.	Definiowane szablony i nadawanie użytkownikom dostępów jedynie do grup które są konieczne do wykonania ich pracy.
		7.1.3 Wymagane udokumentowane pozwolenie na zmiany wydane przez osoby przygotowujące zestaw wymaganych uprawnień.	W 8MAN jest konieczne aby wprowadzić komentarz w przypadku każdej zmiany. Można również dodawać odnośniki do dokumentów.
Zalecenie 8: przydzielenie unikalnego numeru dla każdej osoby mającej dostęp do komputera	8.5 Zapewnić prawidłową identyfikację użytkownika i zarządzanie uwierzytelnieniami dla użytkowników nie będących konsumentami oraz administratorom wszystkich komponentów systemu poprzez:	8.5.4 Natychmiastowe zablokowanie praw dostępu dla dowolnego usuniętego użytkownika.	Poprzez 8MAN możemy miękko usunąć użytkownika, np. poprzez wyłączenie i przeniesieni go do oddzielnej jednostki organizacyjnej, aby zapewnić usunięcie praw dostępu.
Zalecenie 10: śledzenie i monitorowanie wszystkich dostępów do zasobów sieci i danych posiadacza karty	10.2 Zapewnić poprzez wywiady, badania dzienników audytu oraz badaniu ustawień dziennika audytu:	10.2.1 Sprawdzanie i tworzenie dziennika dla wszystkich indywidualnych dostępów do danych posiadacza karty.	Funkcja audytu 8MAN File Server Logga pozwala spełnić to wymaganie.
		10.2.2 Sprawdzanie czy działania podejmowane przez poszczególne osoby z uprawnieniami administratora lub większymi są rejestrowane.	Funkcja audytu 8MAN File Server Logga pozwala spełnić to wymaganie.
Zalecenie 12: Utrzymanie polityk bezpieczeństwa dla całego personelu	12.5 Sprawdzać formalne przyporządkowanie bezpieczeństwa informacji przez Oficera Bezpieczeństwa lub członka zarządu zajmującego się bezpieczeństwem. Uzyskiwać i badać informacje na temat polityk bezpieczeństwa i procedur w celu sprawdzenia czy następujące obowiązki bezpieczeństwa informacji są jasne i formalnie przypisane:	12.5.4 Weryfikacja czy odpowiedzialność za zarządzanie kontem użytkownika i zarządzanie autoryzacjami jest formalnie przyporządkowana.	Za pomocą 8MAN można tworzyć, administrować i usuwać konta użytkowników.
		12.5.5 Sprawdzanie czy odpowiedzialność za monitorowanie i kontrolowanie wszystkich praw dostępu jest formalnie przyporządkowana.	Funkcja raportowania 8MAN FS Logga spełnia to wymaganie.