Jak model chmurowy zmienia zarządzanie fizyczną kontrolą dostępu – przykład impero 360®

Model chmurowy wnosi nową jakość do zarządzania fizyczną kontrolą dostępu – umożliwia scentralizowane tworzenie zasad, ich bieżące egzekwowanie oraz pełną przejrzystość operacji. Choć podobne rozwiązania są wdrażane także lokalnie, chmura pozwala realizować je szybciej, łatwiej i bez konieczności utrzymywania rozbudowanej infrastruktury.

Paweł Błachut

W tym właśnie duchu została zaprojektowana platforma kontroli dostępu impero 360® łącząca dane, procesy i uprawnienia w jednym spójnym systemie. Upraszcza pracę IT, automatyzuje powtarzalne zadania oraz zwiększa szybkość reakcji na incydenty.

Przeniesienie zarządzania kontrolą dostępu do chmury ułatwia codzienne zadania związane z obsługą, a centralizacja i automatyzacja oferowane przez impero 360® wspierają organizacje w spełnianiu wymogów regulacyjnych NIS2 i CER.

impero 360® – co się zmienia, gdy kontrola dostępu przenosi się do chmury?

Według raportu *IBM Cost of a Data Breach 2023*, ponad 80% incydentów naruszenia bezpieczeństwa danych dotyczy środowisk lokalnych i hybrydowych, a czas potrzebny na ich wykrycie przekracza 200 dni. Organizacje, które korzystają z rozwiązań chmurowych i automatyzacji procesów, nie tylko szybciej reagują na zagrożenia, ale też ograniczają związane z nimi koszty nawet o 20%. Wnioski są jednoznaczne: właściwie wdrożona chmura może zapewnić wyższy poziom bezpieczeństwa niż klasyczne rozwiązania *on-premise*.

To istotne także w świetle aktualnych wymagań prawnych – dyrektywy NIS2, KSC i CER narzucają bardzo krótkie terminy zgłaszania istotnych incydentów:

- wstępne ostrzeżenie w ciągu 24 godzin,
- zgłoszenie uzupełniające w ciągu 72 godzin,
- raport końcowy maksymalnie po miesiącu.

Tak rygorystyczne ramy czasowe pokazują, jak ważna jest szybkość reakcji i sprawna obsługa incydentów, czego bez odpowiednich narzędzi nie da się dziś skutecznie zapewnić.

Właśnie w takim podejściu powstało **impero 360® – pierwszy polski system kontroli dostępu oferowany w modelu ACaaS** *(Access Control as a Service)* od Unicard Systems. Platforma działa w środowisku Microsoft Azure, gwarantując przetwarzanie danych w certyfikowanych centrach zgodnych z międzynarodowymi standardami bezpieczeństwa (ISO/IEC 27001, SOC 1/2/3) oraz regulacjami RODO. Wszystkie dane są szyfrowane, a dostęp do nich jest stale monitorowany i szczegółowo rejestrowany.

System działa w środowisku Kubernetes, co zapewnia wysoką dostępność, skalowalność i odporność na awarie. impero 360® obsługuje zarówno pojedyncze lokalizacje, jak i rozproszone środowiska z dziesiątkami oddziałów. Wszystkie aktualizacje oraz kopie zapasowe są realizowane w ramach usługi – bez konieczności angażowania zespołów IT klienta. W praktyce oznacza to mniejsze nakłady finansowe, szybsze wdrożenia i znacznie mniej obowiązków operacyjnych.

Przejście do modelu chmurowego oznacza również większą przewidywalność kosztów. Organizacja korzysta z systemu w modelu subskrypcyjnym, bez konieczności inwestowania w serwery, licencje, utrzymanie sprzętu czy zasoby ludzkie potrzebne do zarządzania środowiskiem.

Jeden system, wiele lokalizacji – jak wygląda centralne zarządzanie dostępem w praktyce?

Wraz z rozwojem organizacji i wzrostem liczby lokalizacji systemy zarządzania dostępem zaczynają wymagać większej koordynacji. W modelu rozproszonym mogą pojawiać się nieścisłości, trudność w utrzymaniu spójnych zasad i ograniczona widoczność tego, co dzieje się na poziomie poszczególnych obiektów. Nawet pozornie proste operacje – takie jak aktualizacja uprawnień – mogą zajmować więcej czasu, niż to konieczne.

Model centralny eliminuje te ograniczenia. Jeden system obsługuje wiele lokalizacji – bez duplikowania konfiguracji, osobnych baz, czy lokalnych wyjątków. Raz wprowadzona zmiana obowiązuje wszędzie, decyzje są egzekwowane w czasie rzeczywistym, a nadzór nad dostępem nie zależy od miejsca, lecz od przyjętej struktury.

W impero 360® wszystkie obiekty, punkty dostępowe, użytkownicy i urządzenia funkcjonują w ramach jednej platformy – dostępnej z poziomu przeglądarki. Administrator może zdalnie i niezależnie od lokalizacji dodawać konta, przypisywać uprawnienia, modyfikować harmonogramy, blokować dostęp, konfigurować ustawienia czytników czy sterowników.

Centralizacja upraszcza również zarządzanie uprawnieniami w zależności od roli w organizacji. Pracownik przypisany do konkretnego działu lub stanowiska automatycznie otrzymuje dostęp do odpowiednich stref. W przypadku zmiany zespołu, projektu lub miejsca pracy nie ma potrzeby ręcznej aktualizacji – wystarczy zmiana danych w systemie HR, a uprawnienia zostają automatycznie odświeżone.

Dzięki temu maleje ryzyko nadania zbyt szerokich uprawnień, utrzymywania nieaktualnych dostępów oraz powstawania luk wynikających z braku synchronizacji systemów.

Automatyzacja, która działa na rzecz bezpieczeństwa

Zarządzanie dostępem nie kończy się na otwieraniu drzwi. W firmach o dynamicznej strukturze – z rotacją pracowników, zleceniami zewnętrznymi i regularnymi zmianami organizacyjnymi – ręczne aktualizowanie uprawnień jest niewydajne. W takich środowiskach automatyzacja staje się koniecznością. impero 360® umożliwia powiązanie kontroli dostępu z rozwiązaniami HR, ERP, BMS, Entra ID, CCTV i SSWiN.

Otwarte API pozwala tworzyć spójne ekosystemy, w których dane użytkowników, zmiany strukturalne czy zdarzenia zarejestrowane w innych systemach bezpieczeństwa są automatycznie odzwierciedlane w uprawnieniach dostępu.

System pozwala także automatyzować operacje związane z obsługą gości, powiadamianiem o zdarzeniach i retencją danych. Portal awizacji umożliwia zdalną rejestrację wizyty, a zgoda na wejście może

być udzielana bezpośrednio przez uprawnioną osobę. Zdefiniowane zdarzenia – np. próba wejścia poza harmonogramem – mogą uruchamiać powiadomienia w czasie rzeczywistym.

System impero 360® a zgodność z wymaganiami NIS2 czy CER

W wielu organizacjach bezpieczeństwo fizyczne i cyfrowe wciąż działają w osobnych silosach. Tymczasem regulacje, takie jak NIS2 i CER, jasno pokazują, że takie podejście nie wystarcza. Ochrona systemów IT musi iść w parze z kontrolą nad dostępem do budynków, pomieszczeń i urządzeń, w których te systemy działają. Choć powszechnie uważa się, że NIS2 dotyczy głównie cyberbezpieczeństwa, unijne wytyczne jasno wskazują, że dyrektywy NIS2 i CER powinny być rozpatrywane łącznie – jako element spójnej polityki zarządzania ryzykiem.

Platforma impero 360® umożliwia scentralizowane zarządzanie dostępem do fizycznych lokalizacji – z rejestracją każdego zdarzenia, identyfikacją użytkownika i możliwością natychmiastowego cofnięcia uprawnień. Co ważne, system reaguje w czasie rzeczywistym, dzięki czemu pozwala skutecznie przeciwdziałać incydentom, a nie tylko je dokumentować.

Zgodnie z dyrektywą NIS2, organizacje objęte obowiązkiem stosowania środków zarządzania ryzykiem muszą m.in. zapewnić ochronę przed dostępem osób nieuprawnionych do zasobów i systemów ICT. CER uzupełnia ten obowiązek, nakładając konieczność zabezpieczenia fizycznych elementów infrastruktury. impero 360® działa dokładnie na tym styku – umożliwia ochronę zasobów cyfrowych i fizycznych w ramach jednej platformy, jednej polityki i jednego procesu.

System wspiera również automatyzację procesów wymaganych przez regulacje, takich jak szybkie wycofywanie uprawnień, audytowalność zmian, integracja z systemami HR, kontrola obecności w strefach z ograniczonym dostępem.

W przypadku audytu lub incydentu organizacja może w ciągu kilku minut wygenerować raport: kto przebywał w danej strefie, kiedy, jak długo, na jakiej podstawie i czy posiadał ważne uprawnienia. Dotyczy to także gości oraz podwykonawców, co ma istotne znaczenie w świetle przepisów CER.

impero 360® działa w trybie offline – nawet w przypadku utraty łączności system nadal kontroluje dostęp i zapisuje wszystkie zdarzenia lokalnie, aby zsynchronizować je po przywróceniu połączenia. To istotne np. podczas testów odporności operacyjnej lub incydentów wymagających utrzymania dostępu bez zakłóceń.

System został także wyposażony w szyfrowanie end-to-end oraz autorski kontroler wspierający protokół OSDP, co zapewnia wysoki poziom bezpieczeństwa transmisji. Dzięki połączeniu oprogramowania z hardware'm własnej produkcji Unicard Systems, impero 360® tworzy spójne i kompleksowe rozwiązanie – opracowane i rozwijane przez polskiego producenta. Gdy rynek zalewają niskokosztowe, często niespójne technologicznie systemy z Azji, coraz więcej organizacji docenia transparentność, lokalne wsparcie i przewidywalność wdrożeń oferowanych przez sprawdzonych dostawców krajowych.

Osoby zainteresowane tematyką NIS2 i CER zapraszamy do udziału w cyklu bezpłatnych webinarów organizowanych przez Unicard Systems. Zachęcamy do rejestracji na www.unicard.pl/webinary-nis2

UNICARD SYSTEMS sp. z o.o.
ul. Zakopiańska 162,
30-435 Kraków
www.unicard.pl