MIGRACJA SYSTEMÓW KONTROLI DOSTĘPU: WYZWANIA, BŁĘDY I DOBRE PRAKTYKI – ROZMOWA Z BARTŁOMIEJEM ZADUMIŃSKIM Z UNICARD SYSTEMS

Migracja systemów kontroli dostępu stała się jednym z najważniejszych wyzwań dla przedsiębiorstw i instytucji modernizujących swoje środowiska bezpieczeństwa. Rosnące wymagania technologiczne, potrzeba integracji z innymi systemami oraz presja na zachowanie ciągłości ochrony sprawiają, że przejście na nowe platformy wymaga precyzyjnego planowania i bezbłędnej realizacji. O tym, jak bezpiecznie przeprowadzać takie procesy, jakie błędy zdarzają się najczęściej i jakie standardy powinny spełniać nowoczesne rozwiązania, rozmawiamy z Bartłomiejem Zadumińskim, kierownikiem Działu Wsparcia i Rozwoju Oprogramowania w Unicard Systems – jednym z liderów rynku wdrożeń systemów bezpieczeństwa.

OiB: Proszę w kilku słowach przedstawić Państwa firmę i obszar jej działalności.

B.Z.: Unicard Systems (dawniej Unicard S.A.) to polska firma z ponad 30-letnim doświadczeniem. Specjalizujemy się w projektowaniu i produkcji zaawansowanych systemów bezpieczeństwa oraz identyfikacji osób, w tym nowoczesnych systemów kontroli dostępu (KD).

Naszym flagowym produktem jest impero 360, pierwszy polski system KD w chmurze. Rozwiązanie odpowiada na potrzeby nowoczesnych organizacji, oferując skalowalność, bezpieczeństwo oraz dostępność niezależnie od lokalizacji.

Wszystkie nasze rozwiązania powstają w Polsce – jako krajowy producent elektroniki i oprogramowania mamy pełną kontrolę nad procesem ich tworzenia. To daje nam kontrolę nad procesem tworzenia i wdrażania systemów. Nasze produkty opierają się w 100% na własnych technologiach.

Dzięki sieci oddziałów na terenie całej Polski, realizujemy i utrzymujemy nawet rozbudowane systemy w różnych regionach kraju. Nasze rozwiązania znajdują zastosowanie w sektorze publicznym, korporacyjnym oraz prywatnym – urzędach, szpitalach, instytucjach publicznych, dużych przedsiębiorstwach czy obiektach infrastruktury krytycznej.

OiB: Jakie najważniejsze czynniki sprawiają dziś, że organizacje decydują się na migrację swoich systemów kontroli dostępu na nowe platformy?

B.Z.: Obserwujemy, że organizacje najczęściej decydują się na zmianę systemu z powodu narastającego długu technologicznego dotychczasowych rozwiązań. Użytkownicy zgłaszają trudności z integracją z innymi systemami, brak aktualizacji, ograniczoną możliwość rozwoju oraz przestarzałe i nieintuicyjne interfejsy.

Coraz większe znaczenie ma także możliwość zarządzania dostępem w sposób zdalny, skalowalny i niezależny od infrastruktury lokalnej. Nowoczesne platformy chmurowe odpowiadają na te potrzeby, oferując większą elastyczność i lepszą dostępność funkcji administracyjnych.

OiB: Z perspektywy operacyjnej, które elementy procesu migracji są najbardziej krytyczne dla zachowania ciągłości ochrony obiektu?

B.Z.: Ingerencja w działający system wymaga starannego przygotowania oraz opracowania scenariuszy postępowania na wypadek zakłóceń na każdym etapie. Planowanie przebiegu migracji uwzględnia nie tylko kolejne kroki wdrożeniowe, ale również warianty pozwalające szybko przywrócić kontrolę w razie niepowodzenia.

Wierzymy, że odporność systemu to nie brak błędów, lecz zdolność do ich bezpiecznego opanowania. Jak ujął to Dr Todd Conklin: „Wytrzymałość systemu to nie brak awarii, a zdolność do bezpiecznego znoszenia porażek."

OiB: Jakie błędy najczęściej popełniają firmy podczas modernizacji systemów kontroli dostępu i jakie mogą być konsekwencje takich zaniedbań?

B.Z.: Jednym z najczęstszych jest traktowanie modernizacji systemu kontroli dostępu jako działania wyłącznie sprzętowego lub informatycznego, bez wcześniejszej analizy procesów organizacyjnych. Brak dokładnej inwentaryzacji istniejących uprawnień, stref bezpieczeństwa czy powiązań z innymi systemami skutkuje wdrożeniem rozwiązania, które nie odpowiada rzeczywistym potrzebom organizacji.

Często pomijany jest również etap testowania, w szczególności scenariuszy awaryjnych i zachowania systemu w sytuacjach granicznych. To z kolei może prowadzić do niekontrolowanych przerw w działaniu systemu, braku dostępu do krytycznych stref lub błędów w rejestracji zdarzeń.

Poważnym problemem jest także niedoszacowanie wymagań dotyczących integracji zarówno z istniejącą infrastrukturą (np. SSWiN, CCTV, BMS), jak i z politykami bezpieczeństwa IT. Brak zgodności z obowiązującymi standardami lub przepisami, takimi jak dyrektywa NIS 2, może narazić organizację na sankcje lub zwiększyć ryzyko incydentów cyberbezpieczeństwa.

Niebezpieczne w skutkach są również próby utrzymania przestarzałych elementów systemu „na siłę", na przykład kontrolerów bez wsparcia producenta lub oprogramowania nieobsługującego aktualnych mechanizmów szyfrowania. Takie podejście z jednej strony ogranicza możliwości rozwoju, z drugiej – znacząco obniża poziom ochrony.

OiB: W jaki sposób Unicard Systems przygotowuje analizę przedwdrożeniową, aby zminimalizować ryzyko przestojów lub luk w zabezpieczeniach?

B.Z.: Analizę rozpoczynamy od konsultacji z klientem. Zbieramy informacje o istniejącej infrastrukturze, sposobie zarządzania dostępem oraz ograniczeniach organizacyjnych i technicznych. Weryfikujemy procedury bezpieczeństwa obowiązujące w obiekcie oraz punkty newralgiczne.

Następnie przeprowadzamy wizję lokalną Oceniamy układ stref, rozmieszczenie urządzeń, istniejące systemy powiązane (np. systemy alarmowe, BMS, CCTV) oraz kanały komunikacyjne. Na tej podstawie tworzymy dokumentację porównawczą ze wskazaniem obszarów do integracji, modernizacji lub wymiany.

Zespół projektowy analizuje zebrane dane i przygotowuje rekomendacje – dobieramy rozwiązania z naszego portfolio lub projektujemy nowe komponenty, jeżeli wymagania odbiegają od standardowych scenariuszy.

W każdym przypadku celem jest zapewnienie płynnego przejścia na nowy system bez zakłóceń w ochronie obiektu. Dlatego jeszcze na etapie przygotowania uwzględniamy plan migracji etapowej oraz warianty awaryjne dla zachowania ciągłości działania.

OiB: Czy migracja systemu kontroli dostępu zawsze wymaga całkowitej wymiany infrastruktury, czy możliwe jest podejście etapowe i hybrydowe?

B.Z.: Zakres migracji zależy od tego, czy modernizujemy już istniejącą instalację Unicard Systems czy wdrażamy nowy system w miejsce rozwiązania innego producenta.

W przypadku aktualizacji naszych narzędzi, w większości sytuacji możliwe jest wykorzystanie istniejącej infrastruktury. Wymiana ogranicza się zwykle do sterowników, jeśli są technologicznie niekompatybilne z nowym oprogramowaniem. Urządzenia wykonawcze, takie jak zwory elektromagnetyczne czy rygle, pozostają najczęściej bez zmian.

W przypadku systemów firm trzecich zakres ingerencji zależy od poziomu ich zamknięcia technologicznego. Niektórzy producenci blokują możliwość integracji z zewnętrznymi

rozwiązaniami, co ogranicza możliwość płynnej migracji. W takich sytuacjach wykorzystujemy istniejące elementy elektromechaniczne, a wymieniamy tylko urządzenia sterujące i komunikacyjne.

Tam, gdzie to możliwe, stosujemy podejście etapowe i hybrydowe, które pozwalają na sukcesywną wymianę systemu bez konieczności wstrzymywania pracy obiektu.

OiB: Jakie standardy bezpieczeństwa i interoperacyjności powinny spełniać nowoczesne platformy, aby migracja była inwestycją długoterminową?

B.Z.: Przede wszystkim nowoczesna platforma kontroli dostępu powinna być oparta na aktualnych technologiach i regularnie aktualizowana – zarówno pod kątem funkcji, jak i bezpieczeństwa. Cykliczne aktualizacje pozwalają na szybkie reagowanie na nowe podatności i zmieniające się wymagania rynkowe.

Istotne jest również przestrzeganie otwartych standardów komunikacyjnych (np. OSDP, Wiegand), co ułatwia integrację monitoringiem, systemami alarmowymi czy BMS. Tego rodzaju interoperacyjność zwiększa elastyczność wdrożenia oraz umożliwia rozwój infrastruktury w przyszłości bez konieczności jej całkowitej wymiany.

Ważnym elementem jest także ergonomia. Nowy interfejs powinien być czytelny, intuicyjny i dostosowany do oczekiwań użytkownika. Przejrzystość panelu zarządzania skraca czas szkolenia i zmniejsza liczbę błędów operacyjnych.

System projektowany zgodnie z aktualnymi dobrymi praktykami (m.in. zasadą minimalnego dostępu, szyfrowaniem transmisji, logowaniem zdarzeń) zwiększa trwałość inwestycji i pozwala lepiej chronić zasoby organizacji w perspektywie kolejnych lat.

OiB: W jaki sposób integracja systemów kontroli dostępu z innymi rozwiązaniami bezpieczeństwa – monitoringiem, SSWiN, BMS – wpływa na złożoność procesu migracji?

B.Z.: Integracja z systemami zewnętrznymi zawsze wymaga dokładnej weryfikacji – zakresu połączeń, sposobu komunikacji (online/offline), wersji oprogramowania, a także typów interfejsów udostępnianych przez producentów. Każdy z tych elementów wpływa na skalę prac oraz możliwości techniczne podczas migracji.

Przejście na nową platformę to również dobry moment, aby ocenić zasadność i efektywność istniejących integracji. Weryfikujemy, które połączenia przynoszą wartość operacyjną i biznesową, a które mogą być uproszczone lub wyeliminowane.

Nowoczesne systemy kontroli dostępu powinny być przygotowane na obsługę rozbudowanych scenariuszy integracyjnych, najlepiej w oparciu o otwarte i udokumentowane API, jak ma to miejsce w impero 360. Takie podejście ułatwia połączenie z systemami CCTV, SSWiN, BMS czy HR oraz zwiększa elastyczność przy przyszłych rozbudowach.

OiB: Jakie znaczenie ma cyberbezpieczeństwo w kontekście modernizacji systemów kontroli dostępu i jakie praktyki rekomendujecie Państwo klientom?

B.Z.: Cyberbezpieczeństwo jest jednym z priorytetowych elementów, które należy uwzględnić przy modernizacji systemów kontroli dostępu. Dlatego rekomendujemy migrację do środowiska chmurowego, które zapewnia znacznie wyższy poziom ochrony niż wiele lokalnych instalacji. W przypadku platformy impero 360 korzystamy z infrastruktury Microsoft Azure, która spełnia międzynarodowe standardy bezpieczeństwa (m.in. ISO/IEC 27001, SOC 2, GDPR, ENS, CSA STAR).

Wśród stosowanych środków ochrony znajdują się m.in. szyfrowanie danych w spoczynku i transmisji, segmentacja zasobów i kontrola dostępu oparta na rolach, logowanie i monitoring zdarzeń, uwierzytelnianie wieloskładnikowe (MFA), czy ciągłe testy penetracyjne i aktualizacje zabezpieczeń.

Dzięki chmurze użytkownik nie musi samodzielnie zarządzać infrastrukturą ani monitorować podatności. Odpowiedzialność za bezpieczeństwo fizyczne serwerowni, dostępność systemu i reakcję na incydenty spoczywa na globalnym dostawcy o potwierdzonym poziomie kompetencji.

OiB: Czy obserwujecie Państwo zmianę oczekiwań klientów w zakresie funkcjonalności nowych platform, np. w kierunku mobilnych identyfikatorów, chmury czy analityki danych?

B.Z.: Zdecydowanie obserwujemy zmianę oczekiwań klientów w kierunku większej automatyzacji oraz elastyczności w zarządzaniu dostępem. Pojawia się zapotrzebowanie na takie funkcje jak wirtualna recepcja, pozwalająca na samodzielną rejestrację gości bez udziału personelu, czy depozytory kluczy, które umożliwiają kontrolowany obieg nośników fizycznych wewnątrz obiektu. Administratorzy oczekują także narzędzi pozwalających na natychmiastowe otrzymywanie powiadomień o zdarzeniach związanych z bezpieczeństwem.

W obszarze identyfikacji zauważalne jest rosnące zainteresowanie kodami QR, które stały się wygodnym rozwiązaniem w przypadku pracowników tymczasowych i gości. To technologia, która przy zachowaniu rozsądnego poziomu bezpieczeństwa pozwala na szybkie i niskokosztowe nadawanie uprawnień dostępu.

Równolegle wzrasta zainteresowanie rozwiązaniami chmurowymi oraz analizą danych dostę-

powych. Organizacje chcą wykorzystywać informacje generowane przez system w celach raportowych, organizacyjnych i optymalizacyjnych. Coraz większe znaczenie ma również zgodność z nowymi regulacjami, takimi jak dyrektywa NIS 2 oraz krajowe przepisy dotyczące cyberbezpieczeństwa, w tym projekt ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Wymagają od podmiotów objętych regulacjami wdrożenia odpowiednich środków ochrony systemów IT i OT, w tym systemów kontroli dostępu, jako elementu infrastruktury krytycznej.

OiB: Jakie trendy technologiczne – Państwa zdaniem – będą w najbliższych latach najbardziej wpływać na sposób, w jaki firmy planują i realizują migracje systemów bezpieczeństwa?

B.Z.: Już teraz obserwujemy rosnące zainteresowanie przenoszeniem systemów bezpieczeństwa do środowisk chmurowych, co otwiera drogę do wdrażania nowych funkcjonalności, automatyzacji oraz zaawansowanej analityki. W Unicard Systems aktywnie pracujemy nad zastosowaniem AI w kontekście systemów KD. Choć na rynku nie ma jeszcze dojrzałych komercyjnie rozwiązań tego typu, dostrzegamy w tej technologii ogromny potencjał, zwłaszcza w zakresie predykcji zdarzeń, adaptacyjnego zarządzania uprawnieniami czy inteligentnego reagowania na nietypowe wzorce zachowań.

Zastosowanie sztucznej inteligencji dodatkowo wzmacnia zasadność migracji do architektury chmurowej, tam gdzie możliwe jest skalowanie zasobów, bieżące aktualizacje i szybka integracja z innymi systemami.

Warto również zwrócić uwagę na rosnące znaczenie regulacji prawnych – jak dyrektywa NIS 2 oraz unijne rozporządzenie CER – zobowiązuje przedsiębiorstwa z sektorów uznanych za istotne do wdrażania zaawansowanych środków cyberbezpieczeństwa, monitorowania dostępów i zapewniania ciągłości działania. Chmura ułatwia spełnienie tych wymagań, ale też dostarcza narzędzia wspierające zgodność z przepisami, takie jak centralne logowanie zdarzeń, analiza ryzyka czy kontrola integralności systemu.

OiB: Bardzo dziękuję za rozmowę.

B.Z.: Dziękuję.