04 (46) / 2024

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: NIS2 – JUŻ ZA CHWILECZKĘ, JUŻ ZA MOMENCIK

Czy jesteśmy gotowi na NIS2? Podmioty, które nie spełnią wymogów, będą musiały się liczyć z dotkliwymi karami finansowymi.

ROŚNIE WARTOŚĆ RYNKU KONTROLI DOSTĘPU

Współczesne systemy kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne i bezpieczne rozwiązania.

SECURITY W HOTELARSTWIE – PERSPEKTYWY

Branża security może odpowiedzieć na wiele nowych wymogów rynku, zapotrzebowanie, a także starych bolączek w hotelarstwie.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

Rośnie wartość rynku kontroli dostępu

Wartość światowego rynku kontroli dostępu wzrośnie z 10,4 mld USD w 2024 r. do 15,2 mld USD w 2029 r. To oznacza, że średnia roczna stopa wzrostu w latach 2024-29 wyniesie ok. 7,8%. Tak twierdzą eksperci firmy badawczej Marketsandmarkets.

Skąd ten wzrost? I czy jest to stały trend, czy raczej chwilowy pik wywołany np. sytuacją geopolityczną? W których branżach można spodziewać się największego wzrostu inwestycji w systemy kontroli dostępu, a w których już jest on wyraźny?

Iwona Krawiec

Biorąc pod uwagę zalety systemów kontroli dostępu, nie dziwi fakt, że zainteresowanie nimi wzrasta. Sektorem, który najwięcej w nie inwestuje, jest przemysł, szczególnie ten najbardziej innowacyjny, bliski idei Przemysłu 4.0, gdzie systemy dostępowe coraz częściej są zintegrowane z innymi cyfrowymi rozwiązaniami stosowanymi przez przedsiębiorstwa. Za sprawą algorytmów AI i uczenia maszynowego możliwe jest bardziej zaawansowane i efektywne zarządzanie dostępem do poszczególnych stref w obiektach zakładów przemysłowych.

Kolejnym sektorem są obiekty infrastruktury krytycznej. Tutaj też nakłady rosną, co nie powinno dziwić. Ma na to wpływ sytuacja geopolityczna. Niezależnie od tego, w której części świata usytuowany jest obiekt IK, każdy nim zarządzający, widząc to, co dzieje się w globalnej wiosce, będzie dążyć do wzmocnienia ochrony. Patrząc na polskie albo szerzej europejskie podwórko, znaczący wzrost inwestycji w zaawansowane systemy kontroli dostępu jest związany z oczekiwaną nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa (w związku z dyrektywą NIS2) i zmianą wymogów dla polskich przedsiębiorstw.

– Firmy w tym sektorze stawiają na systemy, które oferują zaawansowane rozwiązania cybersecurity, integrację z istniejącymi systemami bezpieczeństwa IT i zaawansowane metody uwierzytelniania wieloskładnikowego. Ponadto firmy w tej branży są zainteresowane

» *Niezależnie od tego, w której części świata usytuowany jest obiekt IK, każdy nim zarządzający, widząc to, co dzieje się w globalnej wiosce, będzie dążyć do wzmocnienia ochrony.* «

systemami wspierającymi import certyfikatów autentykacyjnych przygotowanych przez klientów i podpisanych przez zaufane Certificate Authority (CA). Obserwujemy także większe zainteresowanie mechanizmami umożliwiającymi przechowywanie kluczy szyfrujących karty na kontrolerach zamiast czytników (tryb transparenty). Takie podejście zapewnia wysoki poziom bezpieczeństwa, co jest kluczowe dla obiektów infrastruktury krytycznej – zauważa Anna Twardowska z Nedap Security Management.

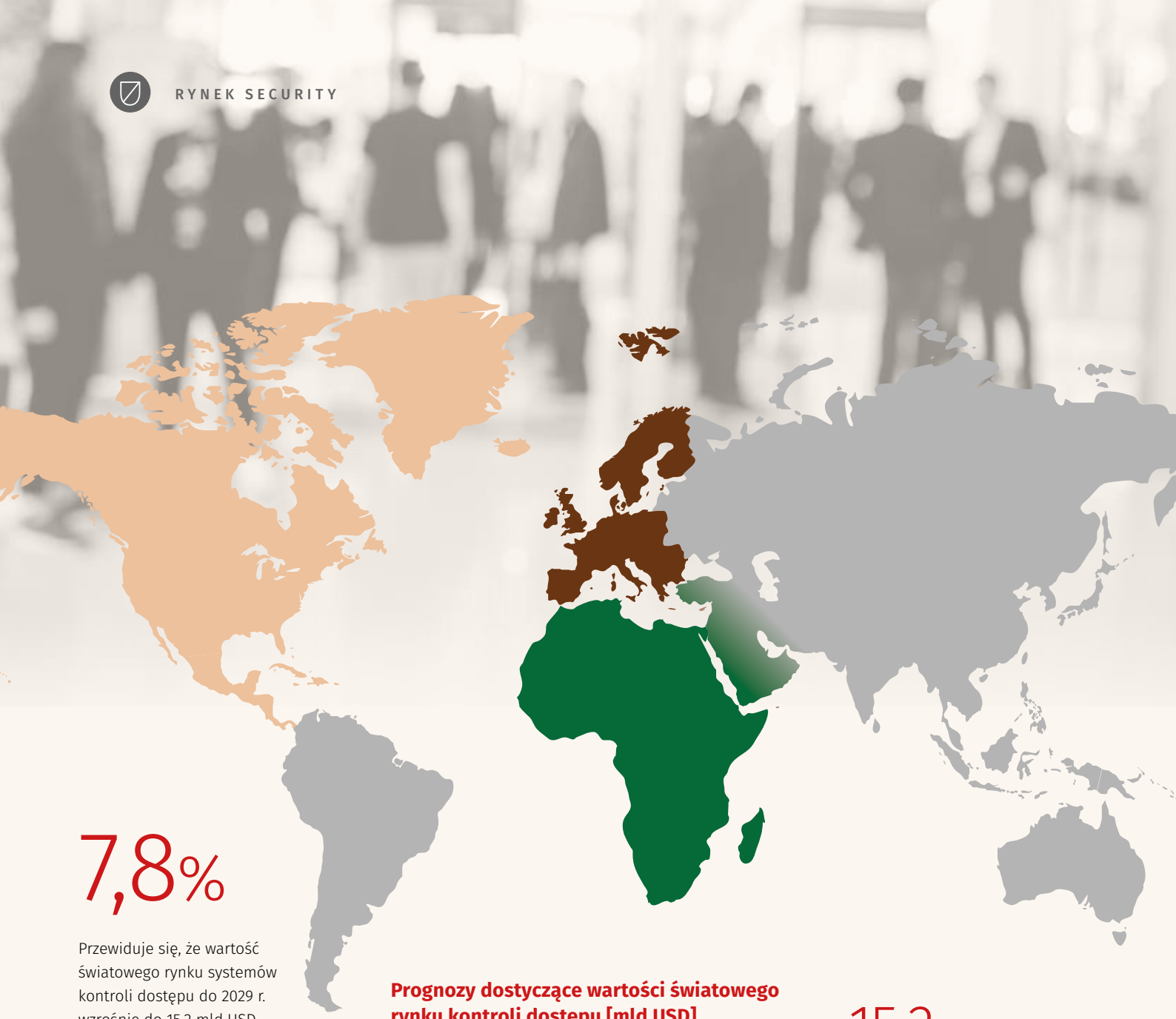
Na potrzebę stosowania rozwiązań wykorzystujących nowoczesne technologie, zwłaszcza w obiektach infrastruktury krytycznej, zwraca uwagę Marek Piotrowski z ZKTeco Europe.

– Od ubiegłego roku wprowadzamy wysoko zaawansowany, zarówno od strony technicznej, jak i zabezpieczeń, system kontroli dostępu ARMATURA (wkrótce z certyfikatem Grade 4). Spowodowało to, że naszymi systemami interesują się firmy z sektora infrastruktury krytycznej, które chcą kompleksowo realizować złożone projekty. To zjawisko nasili się z pewnością jesienią, kiedy wyjdą w życie wymagania postawione dla tego sektora przez NIS-2. Jesteśmy na to przygotowani, tym bardziej że jesteśmy liderami na światowych rynkach, jeśli chodzi o czytniki biometryczne, które gwarantują bardzo wysoki stopień zabezpieczeń – dodaje Marek Piotrowski.

Przeciętnemu użytkownikowi kontrola dostępu kojarzy się przede wszystkim z możliwością wejścia do budynku, np. biurowego. I słusznie. Coraz więcej firm decyduje się na unowocześnienie już funkcjonujących rozwiązań, które mają być jednocześnie elastyczne, łatwe dla użytkowników i skalowalne.

– W sektorze nowoczesnych biur, poza rozwiązaniami cybersecurity, obserwujemy rosnące zainteresowanie rozwiązaniami wykorzystującymi np. Apple Wallet. Jest to odpowiedź na potrzeby klientów, czyli najemców, oczekujących jednocześnie wygody i bezpieczeństwa. Apple Wallet pozwala na łatwe zarządzanie cyfrowymi kluczami dostępu, które można przechowywać na iPhone'ach lub smartwatchach Apple, eliminując potrzebę wprowadzania fizycznych kart dostępu. Organizacje wybierają to rozwiązanie ze względu na jego zaawansowane mechanizmy bezpieczeństwa – komentuje Anna Twardowska.

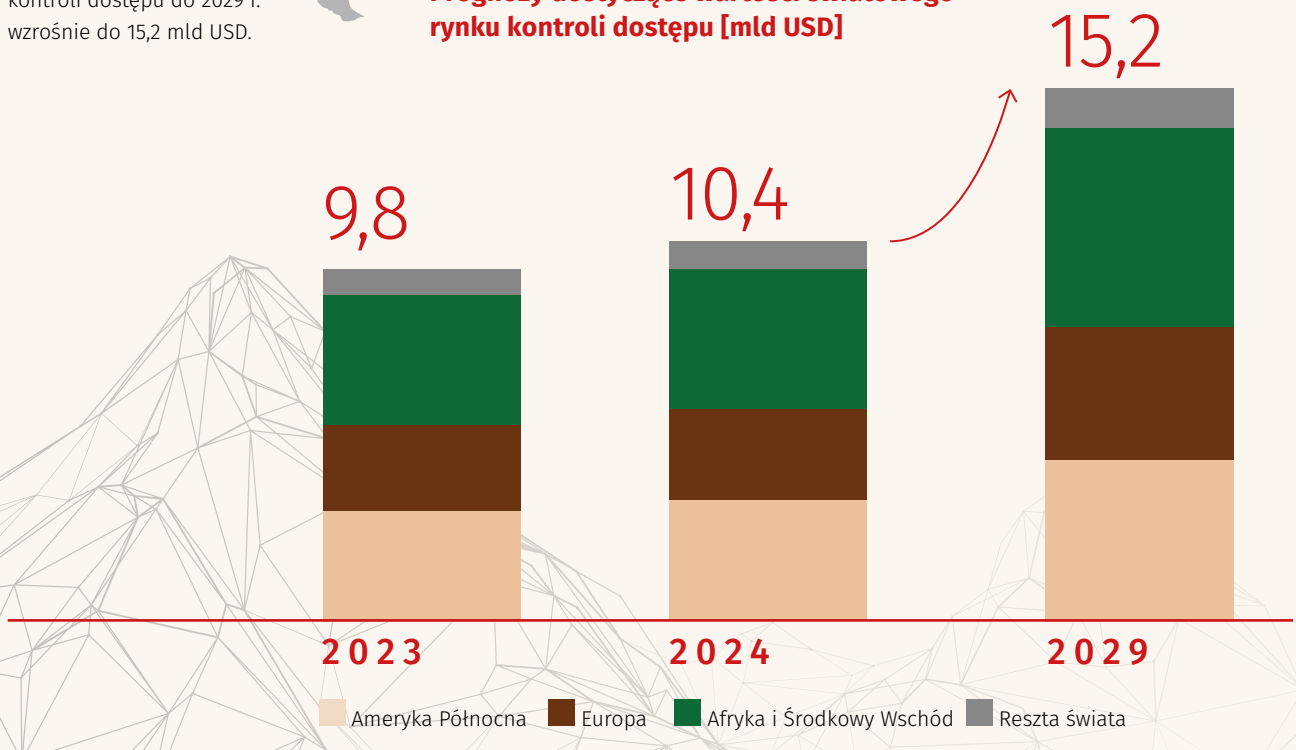
Wspomniana wcześniej globalna wioska korzysta z globalnego transportu. Ten sektor gospodarki zawsze był bardzo ważny, ale chyba dopiero nieszczęsna triada: brexit, pandemia, wojna w Ukrainie dobitnie uzmysłowiły wielu osobom i organizacjom, jak jest ważne, by transport i logistyka działały sprawnie. Ta sprawność wymaga pełnej ochrony łańcucha dostaw. To ważne z uwagi na dużą konkurencyjność w tym sektorze. Z kolei instytucje branży finansowej intensywnie →



7,8%

Przewiduje się, że wartość światowego rynku systemów kontroli dostępu do 2029 r. wzrośnie do 15,2 mld USD.

Prognozy dostyczące wartości światowego rynku kontroli dostępu [mld USD]



Źródło: www.marketsandmarkets.com

rozwijają systemy KD w celu ochrony danych klientów i zapewnienia bezpieczeństwa transakcji.

Sektor hotelarski, podobnie jak inne branże, również musi uwzględniać zmieniające się uwarunkowania geopolityczne, które wpływają na ruch turystyczny, a to na wyniki finansowe. Elastyczność i umiejętność szybkiego reagowania na zmiany stały się kluczowymi cechami skutecznego zarządzania w hotelarstwie. Technologia odgrywa coraz większą rolę w transformacji tego sektora, umożliwiając nie tylko poprawę bezpieczeństwa i komfortu gości, ale także optymalizację procesów operacyjnych i redukcję kosztów.

– Branża hotelowa w coraz większym stopniu kładzie nacisk na wdrażanie rozwiązań zwiększających bezpieczeństwo gości i pracowników oraz samych obiektów hotelowych. Nasi klienci i użytkownicy w szczególności cenią rozwiązania kontroli dostępu, które z jednej strony umożliwiają maksymalne ograniczenie kontaktu bezpośredniego, dzięki wdrożeniu szerokiej gamy rozwiązań opartych na technologii kluczy mobilnych, a z drugiej są w stanie objąć dozorem wszystkie części obiektu hotelowego z poziomu jednej platformy (od pokoi hotelowych, poprzez części konferencyjne i SPA, aż po zaplecze i strefy techniczne). W połączeniu z nowoczesnymi bezpiecznymi kartami i nośnikami zapewnia to najwyższy standard bezpieczeństwa – mówi Przemysław Dawidziuk z Salto Systems.

Te właśnie sektory gospodarki wykazują największą dynamikę w zakresie inwestycji w systemy kontroli dostępu, co wynika z potrzeby zwiększenia bezpieczeństwa i integracji z nowoczesnymi technologiami.

Dominujące trendy

Jak w przypadku każdej dziedziny gospodarki, tak i w sektorze kontroli dostępu da się zauważyć dominujące trendy. Nie dziwi fakt, że są zbieżne z najpopularniejszymi dominującymi na światowym rynku technologicznym. Jednym z nich jest presja na zachowanie integralności danych, które są generowane i gromadzone przez urządzenia kontrolujące, a także odporność na cyberataki tych urządzeń oraz systemów, w których ramach działają.

Każdy komponent systemu dostępowego, począwszy od kart dostępu, przez czytniki, skończywszy na kontrolerach i oprogramowaniu, wymaga szczególnej uwagi. Często nie zdajemy sobie sprawy, że tak wydawałoby się błaha rzecz, jak wybór karty dostępu, może okazać się kluczowa dla zachowania bezpieczeństwa całej firmy. Karta może być najsłabszym elementem, ponieważ można ją klonować i kopiować, a także manipulować nią, a ewentualny atakujący, jeśli wejdzie w jej posiadanie, uzyska wielogodzinny dostęp do zasobów firmy.

– Wybór odpowiednio zabezpieczonej karty, takiej jak Mifare Desfire, Mifare Plus, uniemożliwi skopiowanie karty, ale już niej jej kradzież – zauważa Piotr Karpiński z STid Security. *– Lepszym wyborem będzie karta wirtualna, aktywna po odblokowaniu telefonu biometrią lub FaceId. Takiej karty nie zgubimy, a w przypadku utraty telefonu można ją zdalnie dezaktywować. Dodatkowym atutem jest to, że jest ekologiczna i tańsza od jej plastikowego odpowiednika.*

Jak jednak sprawdzić, czy firma korzysta z rozwiązania odpornego na cyberzagrożenia?

– Kluczowe jest ustalenie wieku systemu lub daty ostatniej wymiany kart. Systemy młodsze niż 10 lat mogą być bezpieczne, o ile karty zostały odpowiednio dobrane. Starsze prawdopodobnie wymagają modernizacji – twierdzi Piotr Karpiński. *– Często też wystarczy do czytnika przyłożyć różne karty kredytowe, bankomatowe czy dowód osobisty. Jeśli czytnik zareaguje, to oznacza albo brak bezpieczeństwa, albo źle skonfigurowany system.*

A jakie rozwiązania zastosować, aby zabezpieczyć firmowy system KD przed cyberatakiem. Bartłomiej Bzymek z firmy Genetec radzi: *– Po pierwsze, wszelkie dane muszą być szyfrowane. Po drugie, przed udzieleniem dostępu do chronionego zasobu tożsamości użytkownika, serwera lub aplikacji klienckiej musi być weryfikowana. Po trzecie, system kontroli dostępu powinien być stale monitorowany pod kątem stanu i pojawiających się aktualizacji. I dotyczy to uaktualnień zarówno czytników, kontrolerów, jak i serwerów oraz jednostek klienckich.*

Integracja z technologiami AI i uczenia maszynowego jest kolejnym wyraźnym trendem. Wykorzystanie sztucznej inteligencji do analizy wzorców dostępu oraz wykrywania anomalii i możliwość szybkiej adaptacji do zmieniających się warunków są bardzo pomocne dla osób zarządzających obiektami.

> *» Współczesne trendy w kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne, elastyczne i bezpieczne rozwiązania. «*

Coraz większą popularność zyskuje biometryczna weryfikacja użytkowników. Najczęściej jest to rozpoznawanie twarzy oraz skanowanie tęczówki oka. Z uwagi na komfort zastosowania wzrasta zainteresowanie użytkowników poświadczeniami mobilnymi. Temu trendowi sprzyjają coraz bardziej zaawansowane smartfony. Wykorzystywanie ich jako kluczy podnosi komfort i elastyczność rozwiązania, w zamian za to redukuje jego koszt, ponieważ nie trzeba drukować kart dostępu, a proces przyznawania uprawnień odbywa się automatycznie. Coraz więcej firm decyduje się także na wprowadzenie systemów kontroli dostępu funkcjonujących w chmurze i przez aplikacje chmurowe zarządzanych. Chmura ma tę zaletę, że zazwyczaj oferuje taką moc obliczeniową, że kontrola nad obiektem może być prowadzona w czasie rzeczywistym.

– Kontrola dostępu w chmurze umożliwia łatwe zarządzanie systemem z każdego miejsca na świecie przez całą dobę. Gwarantuje to użytkownikom wyjątkową mobilność i elastyczność. Priorytetem w naszym systemie jest bezpieczeństwo. Dzięki zaawansowanym technologiom Microsoft Azure zapewniamy solidną ochronę przed nieautoryzowanym dostępem i cyberatakami. Nasi klienci doceniają też niższe niż w przypadku lokalnego systemu koszty początkowe wdrożenia, wygodną płatność subskrypcyjną oraz łatwą integrację z innymi systemami bezpieczeństwa. To znacznie ułatwia zarządzania przedsiębiorstwem – podkreśla Andrzej Mendak z UNICARD Systems.

Współczesne trendy w kontroli dostępu odzwierciedlają rosnące zapotrzebowanie na inteligentne, elastyczne i bezpieczne rozwiązania, które mogą sprostać wymaganiom nowoczesnych organizacji w zakresie ochrony zasobów fizycznych i cyfrowych. Skoro zaciera się granica między światem realnym a wirtualnym, to kompleksowe podejście do bezpieczeństwa, w tym cyberbezpieczeństwa, przestaje być luksusem, a staje się koniecznością. ●