

JAK WYBRAĆ SYSTEM KONTROLI DOSTĘPU

– PRZEGLĄD PRZYDATNYCH FUNKCJI



Sergiusz Parszowski



W tytułowym pytaniu zaszyta jest zarazem pewna trudność, z którą często przychodzi zmierzyć się osobom odpowiedzialnym za przeprowadzenie procesu inwestycyjnego. Na rynku działa bowiem wielu producentów oferujących jeszcze większą ilość systemów kontroli dostępu o różnych parametrach i możliwościach. Oczywistym zatem jest, że musimy zdefiniować sobie kryteria, w oparciu o które dokonamy pewnej selekcji i następnie wyboru tego systemu, który najbardziej będzie odpowiadał naszym potrzebom. W niniejszym artykule chciałbym zwrócić uwagę na jedno takie kryterium, a mianowicie na posiadane przez systemy kontroli dostępu funkcje, które mogą okazać się bardzo przydatne na etapie użytkowania i eksploatacji systemu.

Wprowadzenie

W artykule wymieniam funkcje o różnym charakterze i różnym znaczeniu. Najliczniejszą grupę stanowią te, które bezpośrednio realizują zadania bezpieczeństwa (funkcje bezpieczeństwa). Jednocześnie jednak nie brakuje funkcji, które usprawniają administrowanie systemem (funkcje administracyjne) lub dostarczają dodatkowych korzyści zarządzającym obiektem (funkcje dodatkowe). Opisując poszczególne funkcje będę posługiwał się najbardziej powszechnymi nazwami lub stosował nazwy stworzone przez samego siebie, co nie zmienia faktu, że producenci systemów mogą stosować także inne nazwy techniczne lub marketingowe.

Wybrane funkcje

1. Zbyt długo otwarte drzwi

Jedna z moich ulubionych funkcji. Jeżeli ktoś twierdzi, że nigdy nie widział drzwi przyblokowanych klinem, miotłą czy gaśnicą ... to i tak mu nikt nie uwierzy. Oddzielnie dla każdego drzwi możemy zaprogramować maksymalny czas, przez jaki mogą one pozostawać w pozycji otwartej, zaś przekroczenie tego czasu wyzwala lokalnie sygnał dźwiękowy i wysyła powiadomienie do centrum monitoringu. W przypadkach, gdy drzwi wyposażone są w zamki elektromechaniczne warto stosować dodatkowo kontrolę pozycji rygla i klamki.

2. Zapobieganie podwójnemu przejściu

Jest to funkcja ograniczająca możliwość przejścia więcej niż jednej osobie przy użyciu tego samego identyfikatora, np. przekazanego sobie przez ogrodzenie. Działa to w ten sposób, że jeżeli przykładowo karta dostępu została użyta do wejścia do danej strefy, to nie będzie możliwości użycia jej ponownie do tego samego, jeżeli wcześniej nie zostanie ona użyta do wyjścia z tej strefy. W języku angielskim występuje ona często pod nazwą „anty-pass-back” i ogranicza przypadki tego rodzaju nadużyć.

3. Harmonogramy

Harmonogramy pozwalają z góry określić kto, kiedy i gdzie posiada dostęp. W ten sposób możemy wymuszać przestrzeganie ustalonego czasu pracy i zapobiegać sytuacjom kiedy pracownicy przychodzą zbyt wcześnie do pracy lub pozostają w obiekcie dłużej niż wyznaczony czas. Jest to funkcja pozwalająca przykładowo ograniczać przypadki nadużyć popełnianych ze strony pracowników, którzy pod pozorem zaangażowania wyrządzają szkodę pracodawcy, wymuszając stosowanie obowiązującego czasu pracy czy niedopuszczając do sytuacji, gdy pracownicy przebywają w strefie lub wykonują jakies prace bez wymaganego nadzoru kierownictwa.

4. Wymaganie asysty

Jest to funkcja wymuszająca, by wejście do wyznaczonego obszaru odbywało się zawsze przy najmniej dwuosobowo. Zastosowanie może mieć ona szczególnie w miejscach o podwyższonych wymaganiach bezpieczeństwa, gdzie z racji na wagę chronionych zasobów (np. magazyn, serwerownia, archiwum) lub z uwagi na bezpieczeństwo pracowników (np. pomieszczenia techniczne, sterownicze itp.) wymagane jest zapewnienie stałej asysty co najmniej jednej dodatkowej osoby. Niekiedy działa ona także w połączeniu z regułą „manager first”, gdzie wejście do strefy czy pomieszczenia nie jest możliwe, jeżeli nie jest w niej obecny kierownik odpowiedniego szczebla.

5. Wejście pod przymusem

Jest to ta sama funkcja, którą znamy z systemów sygnalizacji włamania i napadu. Została ona stworzona z myślą o sytuacji, gdy osoba uprawniona do przebywania w danej strefie czy pomieszczeniu jest zmuszana przez osobę nieuprawnioną do otwarcia drzwi pod groźbą użycia przemocy. Wejście pod przymusem umożliwia normalne wejście przy jednoczesnym wygenerowaniu cichego sygnału napadu. W zależności od sposobu zaprogramowania systemu może on tak zareagować przykładowo po wprowadzeniu zmodyfikowanego kodu dostępu (np. pierwsza cyfra kodu podniesiona o „1”) czy też kilkukrotne lub dłuższe przyłożenie identyfikatora do czytnika.

6. Śluzowanie przejść

Funkcja ta pozwala na grupowanie przejść i ustanawianie reguły, że w jednym momencie tylko jedno z nich może być otwarte. Jest to rozwiązanie, które znajduje zastosowanie wszędzie tam, gdzie przykładowo wymagane jest opóźnienie wtargnięcia lub ucieczki napastnika (np. salony jubilerskie) czy występuje potrzeba przeprowadzenia dodatkowej, np. zewnętrznej weryfikacji wchodzących przez operatora monitoringu (np. skarbiec, serwerownia, archiwum). W przypadkach, gdy weryfikacja uprawnień będzie negatywna śluzka może pełnić rolę pułapki zatrzymującej w tym miejscu osobę do czasu przybycia służb interwencyjnych.

7. Limit czasu

Jest to funkcja, która pozwala określić minimalny lub maksymalny czas, przez jaki osoba może przebywać w wybranej strefie czy pomieszczeniu. Nie jest jednak tym samym, co określenie harmonogramu dni i godzin, w których identyfikatory czy przejścia są aktywne. Opisywana funkcja pozwala natomiast kontrolować przykładowo czy ktoś nie przebywa zbyt długo w danym obszarze, co już samo w sobie może być nieprawidłowością lub



może być powodem do sprawdzenia, jakie czynności wykonuje dana osoba (np. w serwerowni). Podobnie limity czasu możemy określać także dla pojazdów dostawców czy serwisów wjeżdżających na chroniony teren.

8. Limit osób

Jest to funkcja, która pozwala określić minimalną lub maksymalną liczbę osób jaka jednocześnie może lub musi przebywać w danym obszarze. W ten sposób możemy przykładowo zapobiegać przepełnieniu jakiegoś obszaru czy opuszczeniu jakiegoś stanowiska pracy bez zapewnienia wymaganego zastępstwa (np. centrum monitoringu). W podobny sposób możemy kontrolować kolejki do przygotowanych atrakcji czy udostępnionych udogodnień i to zarówno w obiektach użyteczności publicznej, jak i w zakładach pracy.

9. Monitoring w czasie rzeczywistym

Jedną z głównych podatności wszystkich systemów kontroli dostępu bazujących na fizycznych identyfikatorach (np. kartach, brelokach itd.) jest to, że wbrew przyjętym w organizacji zasadom, mogą one być przekazywane sobie przez użytkowników. Jeżeli w systemie prezentowane są w czasie rzeczywistym wszystkie przypadki użycia identyfikatorów z jednoczesnym wyświetlaniem zdjęć właścicieli tych identyfikatorów, to w połączeniu z obrazami pochodzącymi z kamer,



operator centrum monitoringu może weryfikować czy danym identyfikatorem postępuje się właściwa osoba.

10. Losowa kontrola

Jest to funkcja, która losowo wskazuje osoby, pojazdy czy transporty do przeprowadzenia dodatkowej kontroli, np. wnoszonych lub wynoszonych rzeczy, postępowania się odpowiednim identyfikatorem, posiadania właściwej karty wjazdowej. W ten sposób możemy również skierować osobę na badanie trzeźwości, sprawdzić ważność pozwoleń czy kompletności wyposażenia, np. środków ochrony indywidualnej. Zastosowanie losowej kontroli pozwala zapewnić wysoką przepustowość wejść przy jednoczesnym optymalnym poziomie bezpieczeństwa obiektu.

11. Ewidencja czasu pracy

Coraz częściej systemy kontroli dostępu pełnią jednocześnie rolę systemu ewidencji czasu pracy. Jestem ogromnym zwolennikiem takiego podejścia, gdzie systemy bezpieczeństwa realizują także poboczne procesy i wspierają codziennie także pozostałe obszary funkcjonowania organizacji. Zazwyczaj zdecydowanie łatwiej jest uzasadnić zakup takiego systemu, większa jest też motywacja, by utrzymywać go w pełnej sprawności oraz łatwiej zarządzać jest tożsamościami pracowników oraz nadanymi im dostęпами.

12. Lokalizacja osób

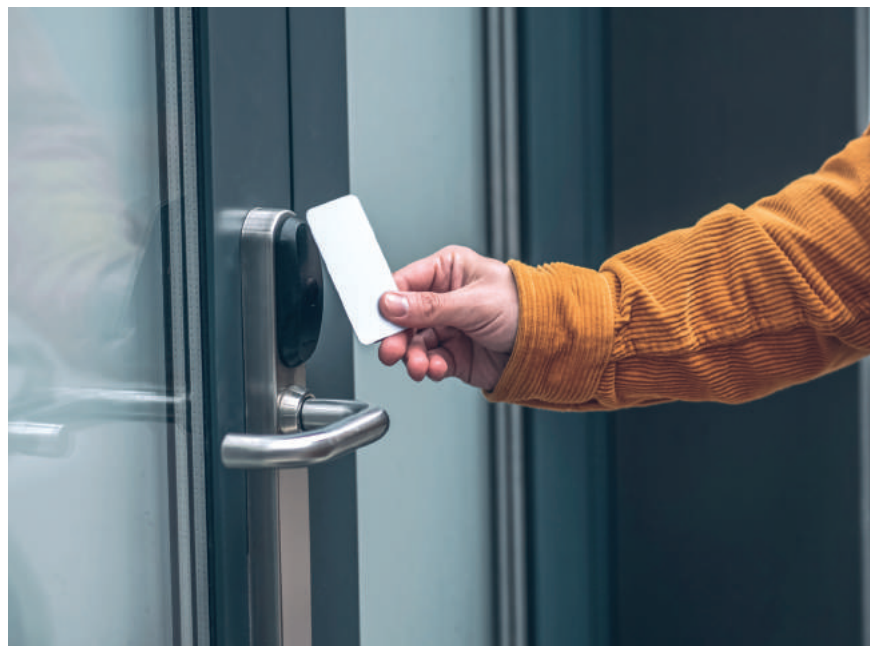
W sytuacjach szczególnych uzasadnionym może być potrzeba szybkiego ustalenia w jakim obszarze może przebywać określona osoba. Funkcja wyszukiwania osób pokaże w jakim obszarze ostatnio przebywała osoba oraz jak przebiegała trasa jaką przebyła ona do tego miejsca. Zastosowanie takiej funkcji może być zasadne przede wszystkim w miejscach wysokiego ryzyka dla zdrowia i życia pracowników, np. zakłady przemysłowe, zakłady energetyczne, kopalnie itp.

13. Lista obecności

Lista obecności pozwala w dowolnym momencie wygenerować listę wszystkich osób znajdujących się na chronionym obszarze. W ten sposób jesteśmy w stanie szybko ustalić ile osób i kto dokładnie przebywa na obiekcie. Natomiast w przypadku wystąpienia pożaru lub innego miejscowego zagrożenia pozwala sprawdzić nie tylko jak dużo osób, ale także kto dokładnie przebywał na zagrożonym obszarze i porównać z listą osób, które stały się w punkcie zbiórki podczas ewakuacji.

14. Bezpieczna ewakuacja

A jeżeli już mowa o ewakuacji to przydatną funkcją może być możliwość tworzenia scenariuszy. W przypadku integracji systemu kontroli dostępu z systemem sygnalizacji pożaru, sygnał wysłany z centrali pożarowej może przykładowo wyzwoić zwolnienie kontroli dostępu na wszystkich drzwiach dróg ewakuacyjnych. W bardziej zaawansowanych systemach kierunek i droga ewakuacji może być natomiast zmieniana w zależności od miejsca, w którym powstało zagrożenie.



15. Trasy dozorowe

Jest to funkcja, która służy kontroli poprawności wykonywania zadań przez pracowników ochrony, podobnie do tego jak to robią dedykowane systemy. W ten sposób możemy wyznaczyć trasy po których mają być realizowane patrole według określonego harmonogramu. Każda niezgodność co do trasy czy czasu realizowanego patrolu powinna być rejestrowana i raportowana, tak bezpośrednio do komórki nadzorującej, jak i przykładowo do zlecającego usługę ochrony (np. pominięcie punktu, zbyt szybki/wolny czas przejścia, rozpoczęcie patrolu zbyt szybko czy zbyt późno).

16. Dłuższy czas otwarcia

W przypadkach, gdy z obiektu korzystają osoby o szczególnych potrzebach system kontroli dostępu wielokrotnie powinien zachowywać się odmiennie od jego domyślnej konfiguracji. Jedną z takich sytuacji jest potrzeba przejścia przez automatycznie otwierane drzwi przez osoby o ograniczonej zdolności poruszania się (np. poruszające się na wózku). Jako, że domyślne czasy otwarcia takich drzwi mogą być niewystarczające, by bezpiecznie i komfortowo przez nie przejść, system powinien umożliwiać nadanie takiemu użytkownikowi specjalnego statusu powodującego odstępstwo od ogólnych reguł i przykładowo wydłużenie czasu otwarcia takich drzwi o dodatkowe 15 sekund.

17. Unieważnianie kart

Jednym z często występujących problemów diagnozowanych podczas audytów bezpieczeństwa fizycznego obiektów jest pozostawianie w systemach kontroli dostępu wielu aktywnych użytkowników, którym to wcześniej przyznane dostępy powinny być ograniczone lub odebrane. Ograniczaniu ilości takich przypadków służy możliwość określania z góry terminu ważności identyfikatorów, wymuszanie okresowego potwierdzania czy przedłużania przyznanego dostępu, automatyczne blokowanie nieużywanych identyfikatorów czy automatyczne blokowanie użytkowników w przypadku planowanej długotrwałej przerwy w wykonywaniu swoich obowiązków (np. długotrwałe zwolnienie lekarskie, urlopy rodzicielskie).

18. Funkcje awizacyjne

Oczekowaną funkcją systemu kontroli dostępu jest możliwość dokonywania awizacji gości, dostaw i serwisów. W ten sposób możliwe jest zautomatyzowanie lub półautomatyzowanie procesów dotyczących przyjmowania zgłoszeń i ich akceptacji, weryfikacji uprawnień i zezwoleń, powiadomienia właściwych komórek, generowania

identyfikatorów, potwierdzania tożsamości, rezerwacji potrzebnych zasobów, czy wreszcie nadzoru nad wizytą oraz rozliczania z czasu pobytu.

19. Reguły awaryjne

W dowolnym momencie funkcjonowania obiektu może wystąpić zdarzenie, które wymusi dynamiczne dostosowywanie działania systemu do aktualnych potrzeb bezpieczeństwa. Wyobraźmy sobie, że potrzebujemy natychmiast zablokować wszystkie drzwi prowadzące do budynku (np. napastnik na zewnątrz), zablokować boczne przejścia wzdłuż określonej trasy (np. przejście VIP-a), czy odblokować wszystkie przejścia podczas innego zagrożenia niż pożar. Możliwość natychmiastowego włączenia wcześniej zaprogramowanych reguł czy scenariuszy, według których od teraz będzie działał system, pozwala błyskawicznie reagować na występujące zagrożenia czy pojawiające się potrzeby.

20. Funkcje analityczne

Wprawdzie funkcjom analitycznym powinno się poświęcić odrębny artykuł, jednak w tym miejscu także na nie chciałbym zwrócić uwagę. Systemy kontroli dostępu naturalnie zbierają ogromne ilości, które przy odpowiedniej wiedzy i umiejętnościach można z pożytkiem wykorzystać. Z punktu widzenia zarządzających obiektem przydatne mogą być chociażby informacje o liczbie osób przebywających w obiekcie/strefach/pomieszczeniach w poszczególnych dniach i godzinach, częstotliwości użytkowania danych przejść, obciążenia poszczególnych udogodnień (np. toalet, kuchni itp.).

Zakończenie

Na zakończenie chciałbym tylko jeszcze raz podkreślić, że kryterium funkcji, choć bardzo ważne, nie może być jedynym brany pod uwagę przez inwestora podczas wyboru systemu kontroli dostępu. Założenia funkcjonalno-użytkowe systemu muszą uwzględniać także założenia dotyczące wielkości systemu, intensywności użytkowania, wymaganego poziomu zabezpieczenia, obowiązujących przepisów prawa czy wymagań organizacyjnych. ■

Sergiusz Parszowski

Lider zespołu eksperckiego Instin.pl

Prezes think tanku ObserwatoriumBezpieczenstwa.pl