JAK INTELIGENTNA KONTROLA DOSTĘPU MOŻE POMÓC W „POWROCIE DO BIURA"

Tłumaczenie Andrzej TOMCZAK

Koniec ograniczeń covidowych oznacza, że w nadchodzących miesiącach większość pracodawców będzie oczekiwać powrotu pracowników do biur i innych zakładów pracy. Wielu z nich uważa, tak jak Elon Musk, że praca zdalna jest mniej wydajna od pracy stacjonarnej. Dwa lata życia z pandemią skłaniają pracodawców i właścicieli firm do przeanalizowania, jak systemy kontroli dostępu mogłyby pomóc w tworzeniu bezpieczniejszego środowiska pracy.

Poniżej kilka wskazówek związanych z dostosowaniem systemów zabezpieczeń do pocovidowej rzeczywistości.

Bezdotykowy i bezproblemowy dostęp dla użytkowników

Zintegrowana kontrola dostępu oznacza dla użytkowników, że mogą bezdotykowo używać kart lub telefonów komórkowych do otwierania drzwi, przywoływania windy, wchodzenia na parkingi, a nawet płacenia za napoje, przekąski i posiłki. Nie potrzebują kluczy ani kodów PIN. Jedna karta lub telefon może otworzyć wszystko, czego potrzebują. Nawet uwierzytelnianie dwuelementowe (ang. *Two Factor Authentication – 2FA*) można zrealizować za pomocą telefonu, więc nadal można stosować bezdotykowo dodatkowe zabezpieczenia, przy minimalnym utrudnieniu dla użytkowników.

Zarządzanie odwiedzającymi i zmniejszanie tłoku w holu budynku

Integracja oprogramowania do zarządzania gośćmi z systemem kontroli dostępu pozwala na to, aby każda firma tworzyła własne przepustki dla gości, bez konieczności korzystania z recepcji budynku. Przepustki mogą być wysyłane do odwiedzających w formie cyfrowej i, wraz z odpowiednim kodem QR, pojawić się automatycznie

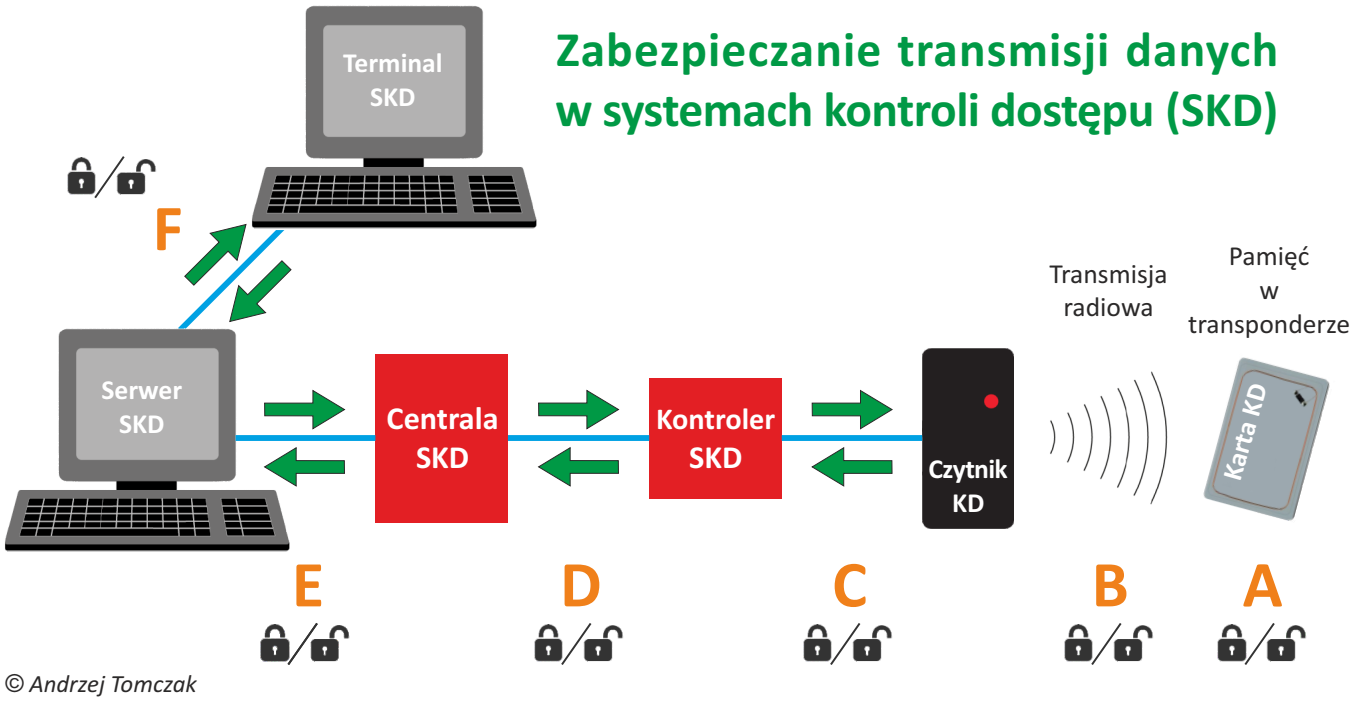
Klasyfikacja stopnia zabezpieczenia
(wg PN-EN 60839-11-1:2014-01, Tablica 1)

Stopień	1	2	3	4
Poziom ryzyka	niski	niski do średniego	średni do wysokiego	wysoki
Zastosowanie	organizacja ruchu, zabezpieczanie zasobów niskiej wartości	organizacja ruchu, zabezpieczanie zasobów niskiej do średniej wartości	w mniejszym stopniu organizacja ruchu, zabezpieczanie zasobów handlowych od średniej do wysokiej wartości	głównie zabezpieczanie bardzo wysokich wartości handlowych albo infrastruktury krytycznej
Umiejętności/wiedza intruzów/atakujących	niski poziom umiejętności, niski poziom wiedzy o SKD, brak wiedzy o identyfikatorach i technologii IT małe środki finansowe na dokonanie ataków	średni poziom umiejętności i wiedzy o SKD, niski poziom wiedzy o identyfikatorach i technologii IT małe do średnich środki finansowe na dokonanie ataków	wysoki poziom umiejętności i wiedzy o SKD, średni poziom wiedzy o identyfikatorach i technologii IT średnie środki finansowe na dokonanie ataków	bardzo wysoki poziom umiejętności i wiedzy o SKD, wysoki poziom wiedzy o identyfikatorach i technologii IT duże środki finansowe na dokonanie ataków
Typowe przykłady	hotele	biura, małe przedsiębiorstwa	przemysł, administracja, obiekty finansowe	obszary wysoce wrażliwe (obiekty wojskowe, rządowe, R&D, obszary produkcji krytycznej)

we właściwym czasie na ich telefonie. Dzięki temu można zapewnić szybki i sprawny dostęp dla odwiedzających, co pomaga zmniejszyć tłok w holu budynku.

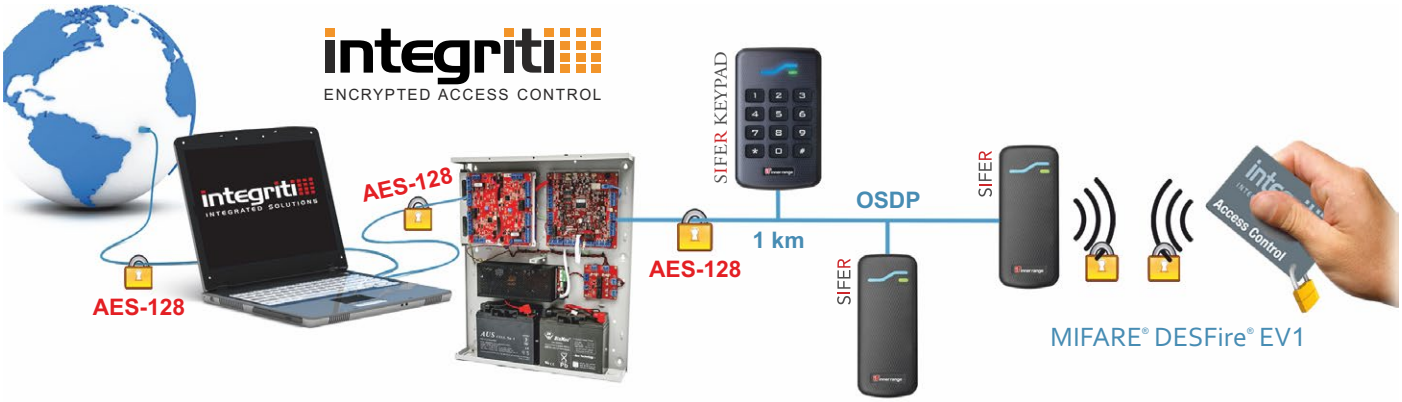
Ograniczanie liczby osób w poszczególnych strefach budynku

Innym sposobem, w jaki systemy kontroli dostępu mogą zarządzać przepływem użytkowników, jest ustalanie limitów osób w poszczególnych strefach budynku. Użytkowników można liczyć np. w całych budynkach, określonych obszarach, poszczególnych biurach lub pokojach, parkingach i windach. Dostęp można ograniczyć po osiągnięciu progu zajętości, aż do uzyskania wolnego miejsca. Wszystkie informacje o zajętości mogą być przesyłane do obsługi w celu monitorowania i ostrzegania, realizowanego w czasie rzeczywistym.



© *Andrzej Tomczak*

Rys. 1. Cyberbezpieczeństwo zależy od szyfrowania danych w newralgicznych punktach systemu kontroli dostępu



Rys. 2. Szyfrowanie End-To-End w systemie Integriti firmy Inner Range

Śledzenie osób i kontaktów

Dobre systemy kontroli dostępu pozwalają zidentyfikować bliskie kontakty osób, u których wykryto objawy choroby zakaźnych, poprzez generowanie szczegółowych raportów o tym, gdzie przebywała zarażona osoba i kto jeszcze był w jej pobliżu.
Raport śledzenia kontaktów może pokazać, przez które drzwi przeszedł zainfekowany użytkownik, ile czasu spędził w każdym obszarze, o której godzinie „wczytał się" na danym przejściu i jacy inni użytkownicy byli w tym czasie w jego pobliżu.

Inteligentne zarządzanie budynkiem

Niezależnie od tego, czy chce się tylko usprawnić zarządzanie oświetleniem, ogrzewaniem i klimatyzacją na podstawie liczby osób znajdujących się w poszczególnych obszarach lub pomieszczeniach, czy istnieje potrzeba zastosowania bardziej wyrafinowanych funkcji, takich jak: sterowanie windami za pomocą interfejsu wysokiego poziomu, zarządzanie gośćmi, integracja z systemem dozoru wizyjnego, wysokiej jakości system kontroli dostępu może zapewnić odpowiednie rozwiązanie. Zarządzający bezpieczeństwem mogą wtedy monitorować i kontrolować wszystkie elementy systemu z jednej, ujednoliconej platformy.

Cyberbezpieczeństwo

Należy oczekiwać, że system kontroli dostępu będzie oferować kompleksowe szyfrowanie w dowolnej wewnętrznej prywatnej sieci komunikacyjnej lub między kontrolerami systemu kontroli dostępu, serwerami i modułami drzwi. (Rys. 1).
Zgodnie z normą międzynarodową, europejską i polską (PN-EN 60839-11-1:2014-01 - wersja polska), dla systemów w stopniach 3. i 4., obowiązkowe jest szyfrowanie komunikacji pomiędzy centralami (kontrolerami) a czytnikami. Systemy w stopniu 3. należy instalować m.in. w obiektach administracji, bankowych i przemysłowych. Natomiast systemy w stopniu 4. należy instalować m.in. w obszarach wysoce wrażliwych takich jak: obiekty infrastruktury krytycznej, wojskowe, rządowe, badawczo-rozwojowe, a także w obszarach produkcji krytycznej oraz w takich, w których zabezpiecza się wartości materialne lub niematerialne o bardzo wysokiej wartości handlowej (Tab. 1).
Najlepsze systemy kontroli dostępu oferują również podział bazy danych na niezależne partycje. Pozwala to na tworzenie wydzielonych przejść kontrolowanych, które istnieją tylko w obrębie partycji, w której zostały utworzone. W ramach partycji można wprowadzać użytkowników z uprawnieniami do wyodrębnionych przejść jak i do grupy przejść wspólnych np. do wejścia do budynku. Partycje bazy danych są całkowicie odizolowane i niewidoczne dla użytkowników innych partycji, takich jak inni najemcy w tym samym budynku, co znacznie zmniejsza szanse cyberprzestępców lub nieuczciwych użytkowników, próbujących uzyskać dostęp do chronionych obszarów i informacji.

Zdalny monitoring

Możliwość zdalnego logowania się osób zarządzającym bezpieczeństwem była niezbędna jeszcze przed pandemią, aby szybko mogli sprawdzić szczegóły w przypadku wystąpienia jakiegoś incydentu. Potrzeba zdalnego logowania wzrosła podczas lockdownu. Po rozluźnieniu przepisów covidowych zdalny dostęp może okazać się potrzebny, gdyby w przyszłości konieczne było przywrócenie ograniczeń.

Integratorzy muszą rozważyć najbardziej elastyczny i bezpieczny zdalny dostęp dla swoich klientów, który może odbywać się za pośrednictwem klienta webowego lub klienta ze stałą lub ruchomą licencją oraz bezpiecznej szyfrowanej sieci VPN lub protokołu tunelowania.
Z praktyki wynika, że zarządzający bezpieczeństwem w dużych biurach lub biurach z wieloma najemcami powinni mieć zagwarantowany zdalny dostęp do systemu za pomocą uprawnionego laptopa lub odpowiedniej aplikacji na telefonie. Pozwala to na elastyczne zarządzanie bezpieczeństwem w sytuacjach krytycznych, które mogą wystąpić również poza godzinami pracy.

Andrzej TOMCZAK
Ekspert Polskiej Izby Systemów Alarmowych, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym