SYSTEMY KONTROLI DOSTĘPU: BEZPIECZNE CZY NIE?

Czy wiesz, że normy od blisko 5 lat zalecają stosowanie szyfrowania?

Andrzej TOMCZAK

W czasie wykładu zwrócono uwagę na następujące zagadnienia:

- Brak zabezpieczeń – zmowa producentów czy potrzeba chwili?
- Dlaczego systemy kontroli dostępu powinny być zabezpieczane?
- Czy wiesz, że normy od blisko 5 lat zalecają stosowanie szyfrowania?
- Czy w najbliższej przyszłości czeka nas wymiana systemów kontroli dostępu?

W czasie konferencji, która odbyła się w trakcie targów IFSEC 2017, wytwórcy urządzeń do systemów kontroli dostępu z rozbrajającą szczerością przyznali, że przez wiele lat wmawiali klientom, że ich systemy świetnie zabezpieczają, nawet szczególnie zagrożone obiekty, a tak naprawdę „wykorzystywane przez nich technologie zatrzymały się na etapie 'wczesnodziecięcym'. Przyznali też, że kodowanie nie było rozwijane – niektórzy do dziś wykorzystują jednokierunkową, niekodowaną transmisję Wieganda i niekodowane karty". Można powiedzieć, że nawet dziś większość producentów do komunikacji pomiędzy czytnikiem a kontrolerem (centralą) korzysta głównie z otwartych, niekodowanych, jednokierunkowych interfejsów Wieganda.

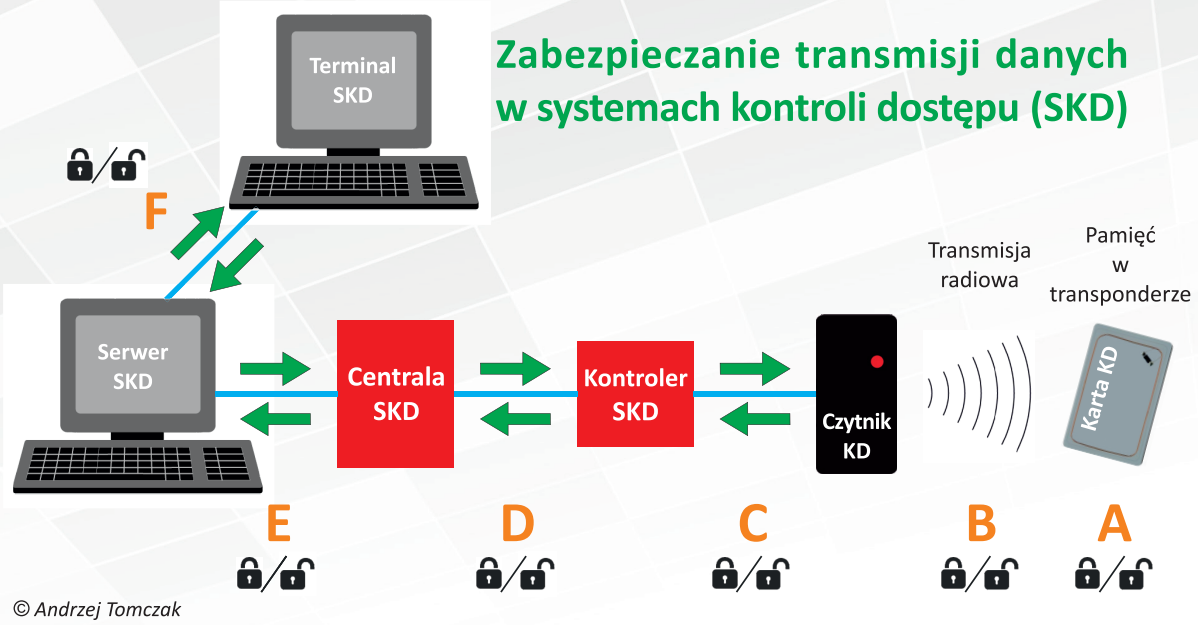
Podstawową przyczyną stosowania otwartego protokołu Wieganda było ujednolicenie metod transmisji, ponieważ producentów technologii czytania jest tylko kilku na świecie, zaś producentów systemów kontroli dostępu jest bardzo wielu. Oprócz tego implementacja jednokierunkowej, niekodowanej transmisji jest dużo tańsza niż dwukierunkowej, szyfrowanej. Żeby zrozumieć, o czym mowa, należy zapoznać się ze schematem blokowym przykładowego systemu, na którym można wskazać „miejsca", gdzie spodziewać się można potencjalnych zagrożeń dla systemów kontroli dostępu (SKD), związanych z transmisją danych. Na rys. 1 zaznaczono literami od A do F miejsca występowania poważnych zagrożeń dla bezpieczeństwa SKD, a tym samym dla chronionego obiektu. Kłódki oznaczają zabezpieczenie lub brak zabezpieczenia, zaś strzałkami zaznaczono kierunek transmisji.

Bardzo wiele systemów, nawet instalowanych współcześnie, nie zostało wyposażonych w jakiekolwiek zabezpieczenia kart i transmisji. Stąd m.in. biorą się, tak ulubione przez inwestorów, niskie ceny. Najniższa cena wydaje się najgorszym doradcą przy wybieraniu systemów kontroli dostępu. Czyli bardzo często firmy oferują niską ceną, fundując klientom „otwarte kłódki" przy literach od A do F – oczywiście nie chwaląc się tym wcale. A skąd klient ma wiedzieć, jaka jest prawda?

Bardzo wiele systemów, nawet instalowanych współcześnie, nie zostało wyposażonych w jakiekolwiek zabezpieczenia kart i transmisji. Stąd m.in. biorą się, tak ulubione przez inwestorów, niskie ceny. Najniższa cena wydaje się najgorszym doradcą przy wybieraniu systemów kontroli dostępu.

BEZPIECZEŃSTWO IDENTYFIKATORÓW

Karta identyfikacyjna została oznaczona na rys. 1 literą A. Karta bezpieczna to taka, która współpracuje tylko z zadeklarowanymi przez użytkownika czytnikami. Trudno jest coś takiego uzyskać, bez wprowadzenia jakichkolwiek zabezpieczeń karty. A niestety większość kart pracujących na częstotliwościach 125 kHz takich zabezpieczeń nie miała. Czym ta przypadłość się objawia? Jeżeli umieścimy taką kartę w zasięgu anteny dowolnego czytnika, generującego sygnał zbliżony



© *Andrzej Tomczak*

Rys. 1. Miejsca występowania poważnych zagrożeń transmisji danych w systemach kontroli dostępu

do 125 kHz, to karta grzecznie odpowiada całą zawartością swojej pamięci. Wystarczy zbliżyć się z ukrytą anteną do osoby posiadającej taką kartę i bez problemu odczytać jej numer, a potem zrobić duplikat karty lub otworzyć przejście bez wykonywania duplikatu, wysyłając odpowiedni sygnał z urządzenia duplikującego (rys. 2).

Najnowsze systemy KD wykorzystują karty pracujące w paśmie przemysłowym na częstotliwości 13,56 MHz, dzięki czemu możliwe jest transmitowanie większej ilości danych niż korzystając z częstotliwości 125 kHz. Ale czy aby na pewno takie karty są bezpieczniejsze? Niestety nie. Niezabezpieczone karty 13,56 MHz duplikuje się za pomocą tego samego urządzenia, pokazanego na rys. 2.

Dlaczego tak jest? Po pierwsze, jeżeli karty 13,56 MHz, czyli większość aktualnie stosowanych kart, są wykonana zgodnie ze standardami ISO/IEC[1], to **obowiązkowo muszą mieć jawny numer seryjny**, nazywany UID[2] lub CSN[3] (rys. 3).

Cóż to oznacza? Że dowolny czytnik, działający zgodnie ze standardami ISO/IEC, może ten numer odczytać. Numer seryjny powinien być unikalny, ale tak nie jest. Elementy elektroniczne kart są produkowane w kilku fabrykach, nie ma więc pewności, że numery seryjne się nie powtarzają. Do tego w niektórych typach kart UID (CSN) można zmienić za pomocą programatora. A informacje wracające z rynku są nieubłagane – zdarzyło się już nie raz, że w tym samym systemie zdublowały się karty. A jeżeli w niektórych typach kart można zaprogramować numer seryjny? Karty, nawet najlepiej zabezpieczone, wykorzystane przez czytniki rozpoznające jedynie UID (CSN) stają się kartami otwartymi, które łatwo można zduplikować. Oczywiście produkowanie urządzeń czytających wyłącznie numer seryjny karty jest bardzo tanie, czyli ulubione przez inwestorów.

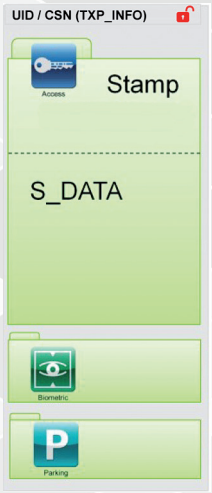
Karty, nawet najlepiej zabezpieczone, wykorzystane przez czytniki rozpoznające jedynie numer seryjny UID (CSN) są niezabezpieczonymi kartami otwartymi.

[1] Grupy normy dotyczących kart to: ISO/IEC 15693, ISO/IEC 14443A i ISO/IEC 14443B.

[2] UID – ang. *Unique Identifier Number.*

[3] CSN – ang. *Card Serial Number.*

Rys. 2. Urządzenie do duplikowania kart: odczyt zawartości pamięci karty i otwarcie przejścia bez produkcji duplikatu karty

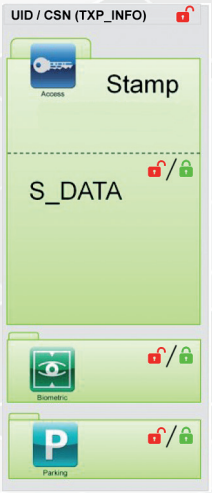


Zgodnie z normami każda karta spełniająca ich wymogi musi mieć niezakodowany numer seryjny karty, nazywany UID (ang. *Unique Identifier Number*) lub CSN (ang. *Card Serial Number*):

- numer ten odczytują czytniki dowolnego producenta, wykonane zgodnie z normami,
- istnieją karty, którym można nadać numer seryjny za pomocą programatora.

Z tego wynika, że istnieje możliwość „podrobienia" numeru seryjnego, czyli „podrobienia" karty do systemu, wykorzystującego do identyfikacji numer seryjny karty UID (CSN)!

Rys. 3. Przykładowy model struktury wewnętrznej karty pracującej na 13,56 MHz – niekodowany numer UID (CSN)



Pozostałe sektory mogą zostać zabezpieczone lub pozostać otwarte, ale dla producenta znacznie tańsze jest niezabezpieczanie sektorów karty.

Z tej prostej, merkantylnej przyczyny wielu producentów nie zabezpiecza sektorów z danymi, które można bez problemu odczytać!

Rys. 4. Przykładowy model struktury wewnętrznej karty pracującej na 13,56 MHz – sektory danych mogą zostać zabezpieczone lub pozostać otwarte

Po drugie, karty potencjalnie bezpieczne mogą nie zostać zabezpieczone. Procedura wykorzystywana przy zabezpieczonych sektorach wygląda następująco: czytnik wysyła kod do odblokowania sektora karty, który chce odczytać, po weryfikacji kodu sektor zostaje otwarty, następuje wymiana informacji, a po skończeniu transmisji – ponowne zblokowanie czytanego sektora (rys. 4). I tak faktycznie działa część systemów, ale wykonanie tej procedury wymaga od producenta dodatkowych, dość skomplikowanych prac informatycznych. A to kosztuje. Bardzo wielu producentów unika utrudniania sobie życia i nie zabezpiecza sektorów w ogóle. Nie trzeba wysyłać kodów odblokowujących czytany sektor. Każdy może ten sektor odczytać, a tym samym nawet teoretycznie najlepsza karta staje się niezabezpieczoną kartą otwartą, którą łatwo skopiować urządzeniem pokazanym na rys. 2. Ale dzięki temu systemy stają tańsze.

> *Nawet najlepsze karty, w których producent nie wykorzystuje dostępnych zabezpieczeń, stają się niezabezpieczonymi kartami otwartymi, tak jak otwarte stają się komputery czy smartfony, w których nie stosujemy procedury uwierzytelnienia użytkownika, np. hasłem.*

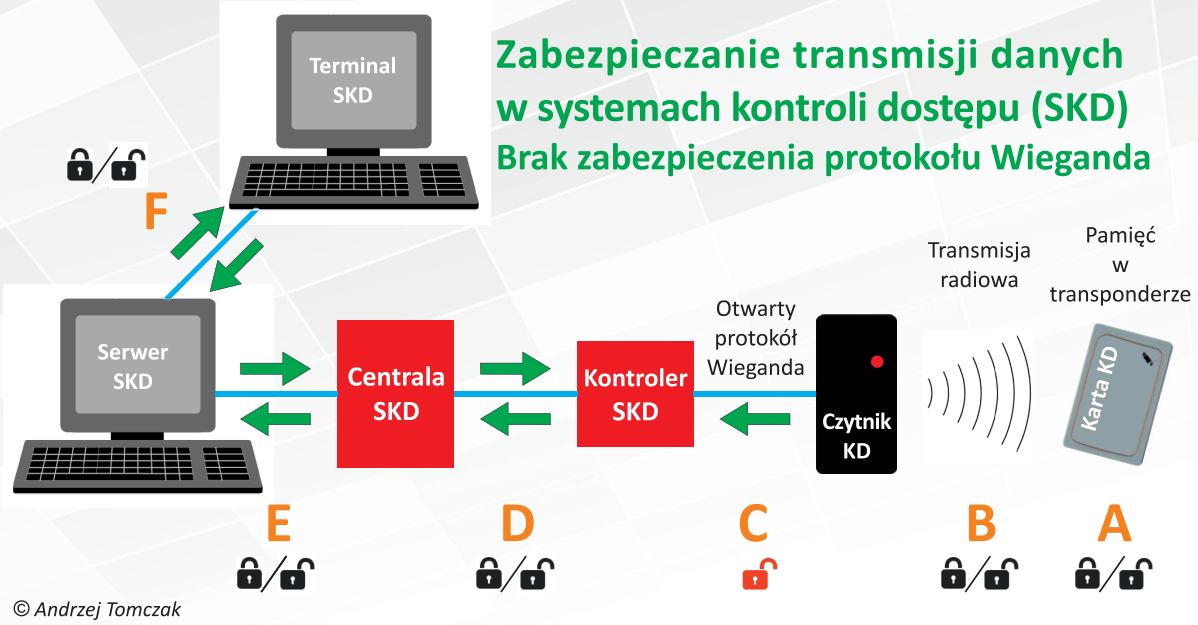
Niestety tej przypadłości inwestor nie ma szans dostrzec, ale fachowcy, których niestety nie ma za wielu w naszym kraju, sprawdzą to bez problemu. I proszę uwierzyć, że na rynku jest całkiem niemało takich systemów, ale za to są tańsze w produkcji. Czyli ich producenci idą zgodnie z rynkowym trendem „najniższej ceny".

KOMUNIKACJA POMIĘDZY CZYTNIKIEM A KONTROLEREM (CENTRALĄ, EKSPANDEREM ITP.)

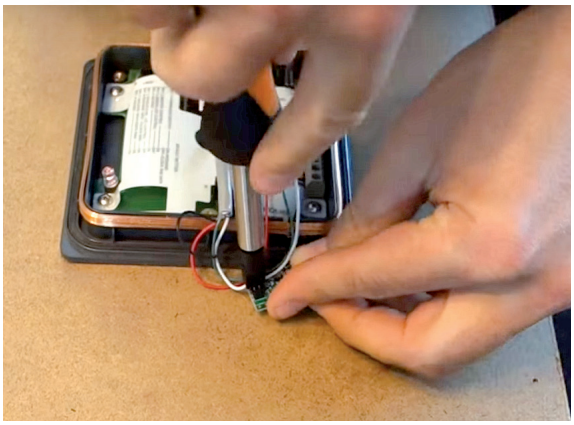
Chodzi tu o komunikację, oznaczoną na rys. 1 literą C. Przypomnijmy stwierdzenie, że „niektórzy do dziś wykorzystują jednokierunkową, niekodowaną transmisję Wieganda". Zastanówmy się nad słowem „jednokierunkowa", czyli wykorzystująca drogę transmisji tylko w jedną stronę – wynika z tego, że powinna na rys. 1 pozostać przy literze C tylko jedna strzałka – w stronę od czytnika do kontrolera SKD (rys. 4). Jakie są tego konsekwencje? Na pewno na karcie nie można wpisywać do sektorów informacji znajdujących się w systemie, ponieważ nie można wysłać żadnej informacji z SKD do czytnika. W prostych systemach KD nie jest to problemem. Skupmy się więc na protokole Wieganda. Jest to protokół niezabezpieczony i dobrze opisany, coś jak dość powszechnie znany alfabet Morse'a. Dlaczego ten protokół na wiele lat zdominował rynek? Odpowiedź jest dość oczywista – potrzebny był prosty, uniwersalny, łatwy do implementacji, a dzięki temu tani sposób komunikacji pomiędzy czytnikiem a kontrolerem. Wspólny, dobrze opisany interfejs rozwiązuje ten problem. Tylko czy aby na pewno jest to bezpieczne? To tak, jakbyśmy w biurach super kodowali wszystkie informacje, czyli – przenosząc to na SKD – np. stosowali bezpieczne karty i komunikację z czytnikami, a następnie komunikowali się ze światem zewnętrznym, stosując ogólnie znany alfabet Morse'a.

Stosowanie transmisji Wieganda naraża właściciela systemu na atak typu „man in the middle". Na czym on polega? Na rys. 5 pokazano montaż urządzenia podsłuchującego transmisję i wysyłającego odczytane numery kart do smartfonu atakującego, za pośrednictwem transmisji Bluetooth. Na tej podstawie można wykonać duplikat karty albo po prostu otworzyć przejście, wydając odpowiednią komendę z aplikacji w telefonie. Komórka wysyła komendę po Bluetooth, a kontroler otrzymuje kod wybranej przez atakującego karty i otwiera przejście, mimo że żadna karta nie została zbliżona do czytnika.

Producenci przyznali się do niekodowania transmisji prawdopodobnie dlatego, że po pierwsze, wejście w życie *Ogólnego rozporządzenie o ochronie danych* (RODO) miało spowodować drastyczny wzrost kar za naruszanie zasad ochrony danych, w tym także zaniedbanie odpowiedniego ich zabezpieczania (np. szyfrowania). Po drugie, opracowany został nowy standard kodowania pomiędzy czytnikami



Rys. 5. Miejsca występowania poważnych zagrożeń transmisji danych w systemach kontroli dostępu – brak zabezpieczeń transmisji pomiędzy czytnikiem a kontrolerem SKD

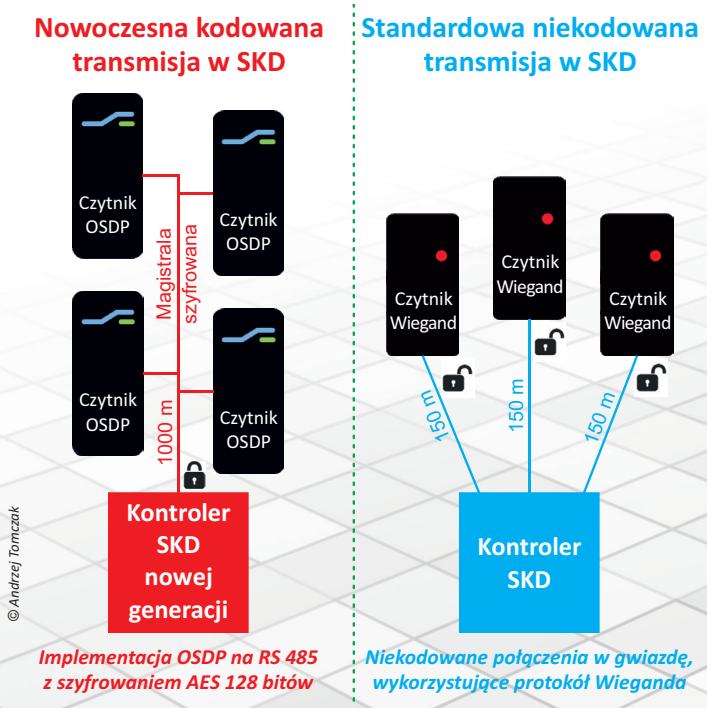


Rys. 6. Montaż urządzenia podsłuchującego transmisję Wieganda, przystosowanego do ataku typu „man in the middle"

a kontrolerami, pod nazwą OSDP[4], wykorzystujący szyfrowanie AES 128 bitów i uwierzytelnianie MAC[5]. Przykłady porównania implementacji systemów z interfejsem Wieganda i OSDP pokazano na rys. 6.

ZABEZPIECZANIE KOMUNIKACJI WEWNĄTRZ SYSTEMU KONTROLI DOSTĘPU

Mowa będzie o transmisji, oznaczonej na rys. 1 literą D. W tym miejscu warto przypomnieć sobie inne seminarium, wygłoszone na IFSEC 2017, pt. *Jak technika cyfrowa przesuwa systemy zabezpieczeń na „ciemną stronę"*. Autor wskazał tam, że systemy wykorzystujące komunikację zamkniętą, nieopartą na sieci komputerowej, gdzie wszystkie urządzenia pochodzą z reguły od jednego producenta, są z reguły dużo lepiej zabezpieczone niż systemy, które wewnątrz wykorzystują komunikację za pośrednictwem sieci Ethernet. Dlaczego? Wyjaśnienie okazuje się proste. „Systemy zamknięte, niesieciowe, mają bezpieczeństwo zagwarantowane przez producenta, zaś w systemach sieciowych bezpieczeństwo w dużej mierze zależy od umiejętności wykonujących i zarządzających tymi systemami. Piętą Achillesa branży zabezpieczeń jest niski poziom edukacji w zakresie tworzenia bezpiecznych sieci komputerowych i zarządzania nimi. Oferujący rozwiązania sieciowe w branży security pomijają milczeniem konieczność tworzenia aktywnych



Rys. 7. Porównanie przykładowych implementacji szyfrowanego standardu OSDP i nieszyfrowanego interfejsu Wieganda

[4] OSDP (ang. *Open Supervised Device Protocol*) – szyfrowany protokół transmisji dla urządzeń peryferyjnych, zob. też https://www.securityindustry.org/SiteAssets/SIAStore/Standards/OSDP_V2%201_5_2014.pdf.

[5] MAC (ang. *Message Authentication Code*) – kod uwierzytelniania wiadomości.

Tabela 1. Klasyfikacja stopnia zabezpieczenia wg PN-EN 60839-11-1:2014-01

Stopień	1	2	3	4
Poziom ryzyka	niski	niski do średniego	średni do wysokiego	wysoki
zastosowanie	aspekty organizacyjne, zabezpieczanie zasobów niskiej wartości	aspekty organizacyjne, zabezpieczanie zasobów niskiej do średniej wartości	mniej aspekty organizacyjne, zabezpieczanie zasobów handlowych od średniej do wysokiej wartości	głównie zabezpieczanie bardzo wysokich wartości handlowych albo infrastruktury krytycznej
doświadczenie/ wiedza przeciwników/ atakujących	małe doświadczenie, mała wiedza o ACS, brak wiedzy o identyfikatorach i technikach IT	średnie doświadczenie iwiedza o ACS, mała wiedza o identyfikatorach i technikach IT	szerokie doświadczenie i wiedza o ACS, średnia wiedza o identyfikatorach i technikach IT	bardzo szerokie doświadczenie i wiedza o ACS, szeroka wiedza o identyfikatorach i technikach IT
	małe środki finansowe na dokonanie ataków	małe do średnich środki finansowe na dokonanie ataków	średnie środki finansowe na dokonanie ataków	duże środki finansowe na dokonanie ataków
typowe przykłady	hotel	biura, małe przedsiębiorstwa	przemysł, administracja, finanse	obszary wysoce wrażliwe (obiekty wojskowe, rządowe, R&D, obszary produkcji krytycznej)

punktów dystrybucyjnych, które powinny być zabezpieczane i zasilane tak, jak inne elementy systemów zabezpieczeń. Trudno o takie zabezpieczenia i gwarancję zasilania, wymaganą dla systemów security, przy wykorzystaniu istniejącej infrastruktury”[6]. Należy pamiętać, że wówczas dla sprawnego i bezpiecznego działania SKD należy zagwarantować bezpieczeństwo fizyczne aktywnych punktów dystrybucyjnych i rezerwowe zasilanie, na wypadek zaniku napięcia sieci energetycznej. A to są dodatkowe koszty, tak nielubiane prze inwestorów. Czyli tego typu zabezpieczenia są najczęściej pomijane, żeby utrzymać się w ulubionym przez inwestorów trendzie „najniższej ceny”. A czy sama komunikacja sieciowa jest bezpieczna? To już zależy od producenta systemu. Oczywiście zawsze taniej będzie nie zabezpieczać tej komunikacji, niż ją zabezpieczyć.

WYBRANE WYMOGI BEZPIECZEŃSTWA OKREŚLONE W AKTUALNYCH NORMACH NA SKD

Nowa norma na systemy kontroli dostępu – PN-EN 60839-11-1 – obowiązuje od 2014 r. Jej tłumaczenie na język polski przeciąga się ze względu na to, że jest to bardzo trudny dokument. Jednak angielskie wersje normy: EN 60839-11-1:2013 i IEC 60839-11-1:2013 obowiązują już od 5 lat. Jedną z charakterystycznych cech tej normy jest wyraźne przypisanie poszczególnych stopni zabezpieczenia do przykładowych obiektów (tabela 1).

Jak widać, ważne obiekty zostały sklasyfikowane w 3. i 4. stopniu zabezpieczenia, a w szczególności obiekty infrastruktury krytycznej zostały przypisane do stopnia 4. Dla SKD w stopniu 4. norma bezwzględnie wymaga stosowanie szyfrowania z uwierzytelnianiem pomiędzy czytnikiem a centralą[7]. Dla stopnia 3. są możliwe dwa rozwiązania: albo szyfrowanie, jak w stopniu 4., albo pełna ochrona antysabotażowa okablowania. Czyli wykorzystanie niekodowanej transmisji Wieganda pomiędzy czytnikiem a centralą KD jest dopuszczalne w 3. stopniu zabezpieczenia, pod warunkiem zastosowania na całej długości przewodów mechanicznej ochrony, ograniczającej możliwość dostępu do linii łączności w celu podsłuchania transmisji lub podłączenia się do niekodowanej linii (np. prowadzenie instalacji w rurkach metalowych z metalowymi puszkami pośrednimi wyposażonymi w ochronę antysabotażową, prowadzenie instalacji w zamykanych i nitowanych metalowych korytach, prowadzenie instalacji pod tynkiem)[8]. Dla stopni 2., 3. i 4. czytniki instalowane na zewnątrz obszaru kontrolowanego lub dostępne z tego obszaru muszą być wyposażone w ochronę przeciwsabotażową.

CO Z TEGO WYNIKA DLA ISTNIEJĄCYCH SYSTEMÓW KD?

W dobie aktualnych zagrożeń terrorystycznych wydaje się wielce prawdopodobne, iż zapisy normatywne staną się podstawą do postawienia wymogów, szczególnie dla krajowych obiektów infrastruktury krytycznej. A postawienie takich wymogów będzie wiązało się na pewno z koniecznością zastąpienia niebezpiecznej komunikacji za pomocą protokołu Wieganda na komunikację szyfrowaną, zgodną z wymogami normy.

[6] *Jak technika cyfrowa przesuwa systemy zabezpieczeń na „ciemną stronę”.* Seminaria i panele dyskusyjne na IFSEC 2017. SEC&AS, nr 4/2017, s. 16–17.

[7] PN-EN 60839-11-1:2014-01, Tablica 7 pkt 24.

[8] PN-EN 60839-11-1:2014-01, Tablica 7 pkt 25.

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym, członek Kolegium Redakcyjnego SEC&AS