CYBERBEZPIECZEŃSTWO A BEZPIECZEŃSTWO FIZYCZNE

Andrzej TOMCZAK

„Bezpieczeństwo fizyczne jest podstawą bezpieczeństwa pracy w sieci. Jeśli osoba atakująca może uzyskać fizyczny dostęp np. do routera, wszystkie poprawki, listy ACL[1] i zestawy funkcji zapory firewall mogą nie chronić sieci. Atakujący może spowodować widoczne lub ukryte uszkodzenia sieci, ponieważ dostęp fizyczny jest poważnym zagrożeniem. Do widocznych uszkodzeń można zaklasyfikować natychmiastowe wyłączenie usług świadczonych przez router, co ma miejsce np. w przypadku kradzieży routera lub jego wyłączenia. Ukryte uszkodzenia są znacznie trudniejsze do znalezienia i poprawienia. Polegają np. na celowym wprowadzeniu złośliwych informacji, które wpływają na usługi routera. Napastnik może przykładowo zmienić jedną linię w wielowierszowej liście ACL, co spowoduje problemy z routingiem. Ta zmiana może prowadzić do godzin, dni, a nawet tygodni spędzonych na śledzeniu problemu routingu”[2].

Ten krótki fragment wytycznych dotyczących zabezpieczania sieci komputerowych świadczy o tym, że bezpieczeństwo fizyczne ma fundamentalne znaczenie dla cyberbezpieczeństwa. Trzeba zdawać sobie sprawę, iż podatność na cyberzagrożenia jest ściśle powiązana m.in. z dostępem fizycznym do elementów sieci komputerowych, nie tylko na poziomie terminalowym, ale również na poziomie urządzeń aktywnych sieci. To, co dla specjalistów od zabezpieczeń jest oczywiste, nie mogło się do tej pory przebić do świadomości krajowej branży IT. Prawdopodobnie dlatego rozporządzenie Ministra Cyfryzacji z dn. 10 września 2018 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usłu-*

[1] ACL (ang. *Access Control List*) – lista kontroli dostępu – to lista uprawnień dołączonych do obiektów takich jak programy, procesy lub pliki. ACL określa, którzy użytkownicy lub które procesy systemowe mają dostęp do obiektów, a także to, jakie operacje są dozwolone na danych obiektach.

[2] Wytyczne dotyczące zabezpieczania routerów Cisco wg National Computer Board.

gi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo tak bardzo poruszyło zainteresowane środowisko.

Bezpieczeństwo fizyczne ma fundamentalne znaczenie dla cyberbezpieczeństwa.

„Cyberprzestrzeń stanowi 'piąty wymiar' walki – obok lądu, powietrza, morza i przestrzeni kosmicznej. […] Pojawiła się nowa kategoria będąca następstwem zmiany podatności i wrażliwości państwa – odporność na zagrożenia cybernetyczne jako wyznacznik bezpieczeństwa państwa"[3]. Działania ofensywne w cyberprzestrzeni są jednym z elementów tzw. wojny hybrydowej. Często zagrożenia hybrydowe są trudno zauważalne, czasami nawet występuje problem, aby je na bieżąco definiować. W kontekście bezpieczeństwa fizycznego i cyberbezpieczeństwa należy zaznaczyć, że do zagrożeń hybrydowych można zaliczyć wprowadzanie do systemów zabezpieczeń urządzeń zawierających rozwiązania oparte na różnego typu oprogramowaniach, pochodzących od producentów spoza krajów „bezpiecznych", szczególnie za naszą wschodnią granicą. Przykładem mogą być systemy kontroli dostępu lub systemy integrujące, od których bezpieczeństwo fizyczne, ale i cyberbezpieczeństwo mogą wprost zależeć. W kontekście tych zagrożeń przyjdzie się również pogodzić z kontrowersyjnym stwierdzeniem, że największe zagrożenia pochodzą z wewnątrz organizacji. I znowu to nic nowego dla specjalistów security – większość poważnych przestępstw jest związana z działaniem lub przynajmniej współudziałem kogoś z wewnątrz organizacji. W przypadku cyberzagrożeń Ponemon Institute, w swoim „Badaniu kosztów zagrożeń wewnętrznych" z 2016 r., ujawnił, że 568 z 874 incydentów naruszających cyberbezpieczeństwo (ok. 65%) było wynikiem zaniedbania bądź rozmyślnego działania pracowników lub kontrahentów. Inne badanie, przeprowadzone przez specjalizującą się w bezpieczeństwie danych firmę Clearswift, wykazało, iż 74% cyberprzestępstw miało swoje źródło wewnątrz organizacji[4].

Mimo twardych danych nie docenia się zagrożenia wewnętrznego, jako mającego podstawowe znaczenie dla bezpieczeństwa.

Czym jest więc bezpieczeństwo? Bezpieczeństwo jest to stan, do którego dążymy. Można zdefiniować wiele rodzajów bezpieczeństwa. Przykładowo, w Narodowym Programie Ochrony Infrastruktury Krytycznej 2018 stwierdza się, że „na działania podejmowane na rzecz zapewnienia bezpieczeństwa składają się:
1) zapewnienie bezpieczeństwa fizycznego,
2) zapewnienie bezpieczeństwa technicznego[5],
3) zapewnienie bezpieczeństwa osobowego,
4) zapewnienie bezpieczeństwa teleinformatycznego[6],
5) zapewnienie bezpieczeństwa prawnego. […]
Zapewnienie bezpieczeństwa fizycznego opiera się m.in. na wykorzystaniu bezpośredniej ochrony fizycznej oraz zabezpieczenia technicznego (elektronicznego i mechanicznego)". Jak widać, istnieje silna współzależność pomiędzy stanem bezpieczeństwa a poszczególnymi jego składowymi. Dla przypomnienia, w rozumieniu ustawy *o ochronie osób i mienia* zabezpieczenie techniczne polega na:
„a) montażu elektronicznych urządzeń i systemów alarmowych, sygnalizujących zagrożenie chronionych osób i mienia, oraz eksploatacji, konserwacji i naprawach w miejscach ich zainstalowania,
b) montażu urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatacji, konserwacji, naprawach i awaryjnym otwieraniu w miejscach zainstalowania".
Należy jeszcze wspomnieć, że zgodnie z nomenklaturą zawartą w Polskich Normach do systemów alarmowych należą m.in. systemy: sygnalizacji włamania i napadu (SSWiN), kontroli dostępu (SKD) i dozoru wizyjnego (VSS/CCTV).

Człowiek jest z reguły najsłabszym ogniwem w systemie zapewnienia bezpieczeństwa.

Jeżeli przyjrzymy się szerzej zagrożeniom wewnątrz organizacji, to łatwo możemy dojść do wniosku, że człowiek jest z reguły najsłabszym ogniwem systemu. Podstawowe wady człowieka związane z zapewnieniem bezpieczeństwa polegają na tym, że człowiek:
- nie może mieć przez cały czas skoncentrowanej uwagi,
- szybko ulega znużeniu,
- męczy się, musi odpoczywać,
- może być pod wpływem alkoholu, środków odurzających itp.,
- łatwo go wyeliminować,
- **może być podatny na korupcję, można go przekupić,**

[3] J. Trybulska, Ł. Wojciechowski: *Bezpieczeństwo państwa w cyberprzestrzeni*. WSEI, Lublin 2017.

[4] IFSEC Global: *Trendy 2018 w systemach dozoru wizyjnego*. SEC&AS, nr 6/2018, s. 26–40.

[5] Bezpieczeństwo techniczne wiąże się z zachowaniem ciągłości produkcji, dostarczaniem mediów, odprowadzaniem ścieków itp. [przyp. red.].

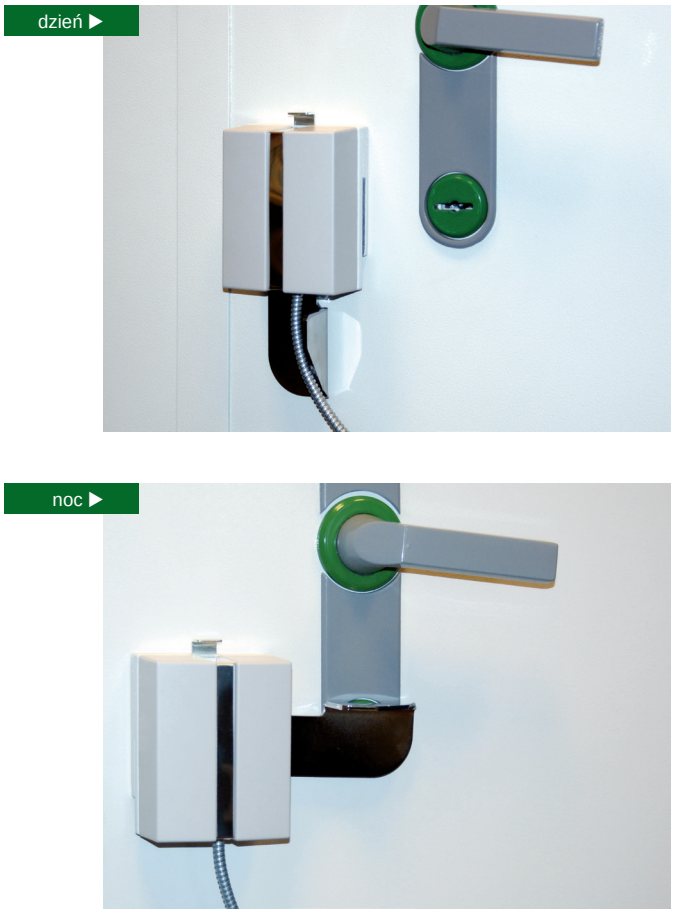
[6] Inaczej: cyberbezpieczeństwa [przyp. red.].

- **można go zastraszyć lub sterroryzować,**
- **często nie przestrzega procedur, np. z rutyny, pośpiechu lub lenistwa!**

Te ostatnie problemy stanowią podstawę do technicznego zabezpieczania infrastruktury sieciowej nawet przed zaufanymi pracownikami, ponieważ „technika" jest „bezdusznym" elementem systemu zapewnienia bezpieczeństwa:

- nie ulega znużeniu,
- nie męczy się, nie musi odpoczywać i spać,
- trudniej ją wyeliminować,
- **nie jest podatna na korupcję, nie można jej przekupić,**
- **nie można jej sterroryzować bądź zastraszyć,**
- **wymusza przestrzeganie procedur!**

Zrozumienie tych problemów jest podstawą tworzenia systemów zabezpieczeń z prawdziwego zdarzenia. Przygotowywanie procedur bezpieczeństwa, które są notorycznie łamane, nie poprawia bezpieczeństwa organizacji – zapewnia tylko dobre samopoczucie zarządzających bezpieczeństwem i ich przełożonych. Analizy ryzyka czy też polityki bezpieczeństwa, opracowywane często zgodnie z zasadą kopiuj–wklej, po tylko, aby coś było zapisane, z reguły niewiele wnoszą w sytuacji realnych zagrożeń. Dlatego warto potraktować „technikę" jako narzędzie wymuszające realizowanie opracowanych procedur.



Rys. 1. Czujka sejsmiczna zamontowana na drzwiach, wyposażona w przestawianą zasłonę dziurki od klucza

Prostym przykładem, jak technika wpływa na przestrzeganie procedury zamykania sejfów (szaf metalowych), łącznie z wyjęciem klucza z zamka przed wyjściem z pracy, jest rozwiązanie pokazane na rys. 1. W szafie została zamontowana czujka otwarcia, a na drzwiach czujka sejsmiczna, wyposażona w przestawianą zasłonę dziurki od klucza.

Wyjęcie klucza z zamka sejfowego jest możliwe tylko w jednym położeniu – przy wysuniętych elementach ryglujących. Jeżeli taki zestaw czujek podłączymy do systemu SWiN, to pracownik nie uzbroi systemu, jeżeli:

- nie zamknie drzwi sejfu (co kontroluje czujka otwarcia),
- nie przekręci klucza w zamku, ryglując drzwi (inaczej nie wyjmie klucza),
- nie wyjmie klucza (inaczej nie zasłoni dziurki od klucza, co jest, obok zamkniętych drzwi, warunkiem koniecznym do uzbrojenia systemu).

Jeżeli system został uzbrojony, wynika z tego, że sejf został prawidłowo zamknięty, a klucz usunięty z zamka. Oczywiście próba odsłonięcia dziurki od klucza bez rozbrojenia systemu SWiN spowoduje alarm. Można wymyślać wiele sposobów wymuszania przestrzegania procedur za pomocą rozwiązań technicznych. Na pewno jedną z ważniejszych będzie procedura komisyjności, czyli zasada czworga oczu.

Jak w powyższym kontekście eksperci PISA oceniają rozporządzenie Ministra Cyfryzacji z dn. 10 września 2018 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*? Mimo szeregu mniejszej lub większej rangi uwag oceniamy to rozporządzenie bardzo wysoko. Obok rozporządzenia Ministra Spraw Wewnętrznych i Administracji dotyczącego przechowywania i transportowania wartości[7] oraz rozporządzenia Rady Ministrów *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych*[8] jest kolejnym kamieniem milowym w porządkowaniu stosowania w naszym kraju środków służących do zapewnienia bezpieczeństwa fizycznego, a jednocześnie również cyberbezpieczeństwa. Niektóre zapisy są tak silne, jak wymóg osiągnięcia przez system dozoru wizyjnego rozdzielczości 400 linii telewizyjnych. Na ten temat można przeprowadzić kilkugodzinny wykład. Tak samo wymagające są określenia „RC2" i „RC4", użyte w omawianym rozporządzeniu. Wprowadzenie takich wymogów kończy dyskusję na temat odporności

[7] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dn. 7 września 2010 r. *w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne*. Dz.U. 2010, nr 166, poz. 1128.

[8] Rozporządzenie Rady Ministrów z dn. 29 maja 2012 r. *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych*. Dz.U. 2012, poz. 683.

przejść w systemach kontroli dostępu. Nasuwa się od razu pytanie, czy w takich przejściach można stosować zwory elektromagnetyczne lub elektrozaczepy jako aktywatory przejścia kontrolowanego. Odpowiedź jest krótka – nie[9]. Jeżeli przejście ma mieć klasę odporności RC, to najprostszym rozwiązaniem jest zastosowanie odpowiednio sklasyfikowanego zamka elektromechanicznego, zamontowanego z adekwatnymi okuciami.

SYSTEMY DOZORU WIZYJNEGO

Analizę rozporządzenia Ministra Cyfryzacji (MC) zacznę od tego, czego w nim zabrakło. Zdaniem ekspertów PISA brakuje zapisów dotyczących systemów dozoru wizyjnego, nazywanych w skrócie VSS[10] lub CCTV[11]. W związku z wejściem w życie przepisów RODO stosowanie systemów dozoru wizyjnego (VSS/CCTV), niepoprawnie nazywanych w przepisach systemami monitoringu, jest utrudnione ze względu na to, iż wizerunek osób należy do danych osobowych, podlegających ochronie. Zapisanie konieczności stosowania systemów dozoru wizyjnego w rozporządzeniu ułatwiłoby procedury ich wdrożenia. Dla przypomnienia odpowiedni zapis Kodeksu pracy: „Art. 22^2. § 1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring)". Stosowanie dozoru wizyjnego, pozwalającego na obserwację kluczowych miejsc oraz pracowników, ma niebagatelne znaczenie dla zachowania cyberbezpieczeństwa. Brak zapisu w rozporządzeniu powoduje konieczność podciągnięcia stosowania dozoru wizyjnego dla zachowania cyberbezpieczeństwa pod jeden z celów określonych w Kodeksie pracy. Czy ma to być: ochrona mienia, kontrola produkcji, bezpieczeństwo pracowników, czy też zachowanie w tajemnicy informacji?

Jeżeli nie stosuje się systemów VSS/CCTV, należy bezwzględnie wprowadzić procedury komisyjności (zasada czworga oczu), kontrolowane i sterowane przez środki techniczne – np. działające tak, że alarm jest wywoływany w momencie, gdy w kontrolowanym pomieszczeniu pozostaje tylko jedna osoba. Możliwość stosowania systemów VSS/CCTV opisano np. w pkt 10 zał. 1 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 2010 r., dotyczącego przechowywania i transportowania wartości:

> „10. W zależności od poziomu ryzyka systemy sygnalizacji włamania i napadu należy uzupełniać o systemy telewizji dozorowej oraz o systemy kontroli dostępu".

W przypadku rozporządzenia MC można wzorować się na tym przepisie:

> *§ 2.1. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo są obowiązane dysponować prawem do wyłącznego korzystania z pomieszczeń, które wyposażone są w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej w:*
> […]
> *2a) systemy dozoru wizyjnego z rejestracją, obserwujące obszary kluczowe dla cyberbezpieczeństwa oraz pracę osób mających wpływ na cyberbezpieczeństwo, z rejestratorami oraz nośnikami zabezpieczonymi przed zniszczeniem i dostępem osób nieupoważnionych.*

Albo rozszerzyć zapis, pozostając w zgodności z pozostałymi wymogami rozporządzenia MC, pisząc:

> *2a) systemy dozoru wizyjnego stopnia 3 według Polskiej Normy PN-EN 62676-1-1 z rejestracją, obserwujące obszary kluczowe dla cyberbezpieczeństwa oraz pracę osób mających wpływ na cyberbezpieczeństwo, z rejestratorami oraz nośnikami zabezpieczonymi przed zniszczeniem i dostępem osób nieupoważnionych.*

Należy zastanowić się nad tym, jak obserwować pomieszczenia. Można to robić, tak jak pokazano na rys. 2 – z podglądem wykonywanej pracy lub bez podglądu ekranów monitorów i klawiatur. To już pozostaje w sferze decyzji zarządzających jednostką, opisanych i umotywowanych w polityce bezpieczeństwa. Ważne jest również odpowiednie fizyczne zabezpieczenie rejestratora przed dostępem osób niepowołanych oraz niepodłączanie go do sieci komputerowej, która mogłaby być celem cyberataku. Wróćmy do podpunktów, tym razem tych, które zostały zapisane w § 2.1 rozporządzenia.

SYSTEMY SYGNALIZACJI WŁAMANIA I NAPADU

Tekst rozporządzenia proponowany przez PISA:

> *1) system sygnalizacji włamania i napadu **stopnia** 2 według Polskiej Normy PN-EN 50131-1* […].

W przypadku systemów sygnalizacji włamania i napadu (SSWiN) i systemów kontroli dostępu (SKD) – dotyczy ppkt 2 – niepoprawnie użyto w rozpo-

[9] Więcej na ten temat w artykule A. Tomczaka: *Zamki elektromechaniczne. Niedoceniany standard zamknięć w systemach kontroli dostępu i ewakuacji*. SEC&AS, nr 2/2019, s. 30–36.

[10] VSS – ang. *Video Surveillance System*.

[11] CCTV – ang. *Close Circuit Television*.

Rys. 2. Obserwacja osób odpowiedzialnych za cyberbezpieczeństwo: z ew. podglądem wykonywanej pracy lub bez podglądu wykonywanej pracy

rządzeniu słowo „klasa". W słownikach aktualnych norm występuje pojęcie: „stopień" (ang. *grade*), a nie klasa.

W kontekście ppkt 1 przypomnę zapisy zał. 1 do rozporządzenia dotyczącego przechowywania i transportowania wartości:

„5. Określa się następujące rodzaje czynności, jakie powinien wykrywać system sygnalizacji włamania i napadu w zależności od stopnia zabezpieczenia: […]

5.2. Stopień 2:

– otwarcie drzwi, okien i innych zamknięć chronionego obszaru,
– poruszanie się w chronionym obszarze (pułapkowo). […]

6. System sygnalizacji włamania i napadu powinien być wykonany co najmniej w 2. stopniu zabezpieczenia i zapewniać identyfikację użytkowników włączających i wyłączających system lub jego część".

Warto również wiedzieć, jakie są dodatkowe konsekwencje wymagania wykonania systemu SWiN w 2. stopniu, wynikające z PN-EN 50131-1:2009. Jest to opisane w Tablicy 10 normy – systemy wykonywane w min. 2. stopniu zabezpieczenia muszą być obowiązkowo podłączone do alarmowego centrum odbiorczego (ACO), nazywanego często stacją monitorowania alarmów lub centrum monitorowania alarmów.

Systemy SWiN wykonywane w min. 2. stopniu zabezpieczenia muszą być obowiązkowo podłączone do alarmowego centrum odbiorczego (ACO), nazywanego często stacją monitorowania alarmów lub centrum monitorowania alarmów.

SYSTEMY KONTROLI DOSTĘPU

Tekst rozporządzenia proponowany przez PISA:

2) system kontroli dostępu ***stopnia 3*** *według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia* ***na podstawie zdefiniowanych w normie danych identyfikacyjnych posiadanych*** *przez tę osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem,* ***wyposażony w rezerwowe źródło zasilania, podtrzymujące działanie systemu po zaniku napięcia zasilania z sieci energetycznej przez okres wynikający z analizy ryzyka*** […].

Zmiana zapisów została przygotowana wg tłumaczenia normy PN-EN 60839-11-1, które aktualnie jest zatwierdzane w KT52 przy Polskim Komitecie Normalizacyjnym. Temat „stopnia", a nie „klasy" został już omówiony. Do tematu stopnia zabezpieczenia jeszcze wrócimy. W kwestii przyznania dostępu sugerujemy zmianę treści, zgodną z zapisami normy, wykorzystując pojęcia „dane identyfikacyjne" (ang. *credentials*), zamiast „posiadanej rzeczy". Poniżej definicja z przetłumaczonego słownika normy PN-EN 60839-11-1:

„3.42 DANE IDENTYFIKACYJNE
informacja zapamiętana lub przechowywana w identyfikatorze

PRZYKŁAD: Informacja zawiera obraz biometryczny wykorzystywany w systemie kontroli dostępu do identyfikacji osoby, w celu uwierzytelnienia użytkownika".

Ponieważ stopień 2. jest najniższym stopniem sugerowanym do obiektów innych niż hotele, a dla obiektów infrastruktury krytycznej norma wskazuje wprost wykonywanie systemów w stopniu 4., naszym zdaniem należałoby podnieść wymagania dla SKD do min. 3. stopnia. Dodatkowo dla SKD w 2. stopniu zabezpieczenia nie ma wymagania zainstalowa-

nia rezerwowego źródła zasilania – po wyłączeniu zasilania sieciowego SKD wykonany w stopniu 2. może przestać działać. Nie oznacza to, że naciskamy na zmianę wymaganego stopnia zabezpieczenia w systemach KD, ale taki wybór wydaje się logiczny. Karty stosowane w 2. stopniu zabezpieczenia nie muszą być zabezpieczone przed nieautoryzowaną modyfikacją, a transmisja między nimi a czytnikami oraz między czytnikami a kontrolerami – szyfrowana. Rozwiązania czytników w 2. i 3. stopniu nie odbiegają cenowo od siebie – w 2. stopniu można natomiast stosować przestarzałą, jednokierunkową, niekodowaną transmisję pomiędzy czytnikiem a centralą (kontrolerem), a w 3. stopniu transmisja powinna być szyfrowana. Ceny czytników tej samej klasy z szyfrowaną i nieszyfrowaną transmisją są podobne (producent wgrywa oprogramowanie z nieszyfrowanym lub szyfrowanym protokołem transmisji), a więc wydaje się, że nie powinno się już „promować" rozwiązań przestarzałych, wprowadzonych standardem z 1996 r., nieuwzględniających szyfrowania, tylko rozwiązania wprowadzone standardem z 2011 r., który zostanie opublikowany jako Polska Norma PN-EN 60839-11-5[12]. Należy zwrócić uwagę na to, iż w rozporządzeniu jest mowa o rzeczywistych klasach zabezpieczenia drzwi (RC2 i RC4), niekorespondujących z określeniem użytym w normie dla stopnia 2.: „organizacja ruchu", która wskazuje na administracyjny (porządkowy, a nie zabezpieczeniowy) charakter przejść kontroli dostępu.

W tabeli 1 (z tłumaczonej normy PN-EN 60839-11-1) wskazano podstawy wyboru stopni zabezpieczenia.

Można ew. zaproponować rozwiązanie pośrednie:

2) system kontroli dostępu ***stopnia*** *2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia* ***na podstawie zdefiniowanych w normie danych identyfikacyjnych posiadanych*** *przez tę osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem,* ***pod warunkiem stosowania identyfikatorów zabezpieczonych przed nieautoryzowaną modyfikacją, szyfrowanej, dwukierunkowej transmisji z uwierzytelnianiem pomiędzy identyfikatorami a czytnikami i kontrolerami oraz wyposażenia systemu w rezerwowe źródło zasilania, podtrzymujące działanie systemu po zaniku napięcia zasilania z sieci energetycznej przez okres wynikający z analizy ryzyka****.*

SZAFY DO PRZECHOWYWANIA DOKUMENTÓW LUB NOŚNIKÓW

Tekst rozporządzenia proponowany przez PISA:

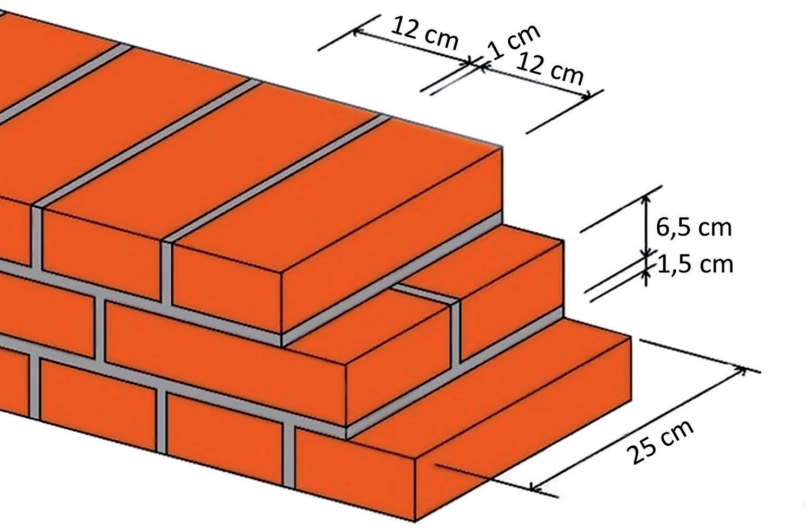
4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych o istotnym znaczeniu dla prowadzonej działalności klasy S1, spełniającymi wymagania Polskiej Normy PN-EN 14450, ***a jeżeli na podstawie przeprowadzonego szacowania ich zastosowanie rodziłoby nieakceptowalne ryzyko dla przechowywanych dokumentów lub informatycznych nośników danych, związane z zagrożeniem pożarowym, szafy służące do przechowywania dokumentów klasy LFS 60 P wg PN-EN 15659 lub szafy służące do przechowywania informatycznych nośników danych klasy S 60 DIS wg PN-EN 1047-1****, chyba że inne przepisy wymagają wyższych klas odporności szaf* […].

[12] Zob. też IFSEC Global: *Cała prawda o szyfrowanym protokole komunikacyjnym OSDP*, SEC&AS 2/2019, s. 38.

Tabela 1. Klasyfikacja stopnia zabezpieczenia

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 ACS*, brak wiedzy o identyfikatorach i technologii IT małe środki finansowe na dokonanie ataków	średni poziom umiejętności i wiedzy o ACS, niski poziom wiedzy o identyfikatorach i technologii IT małe do średnich środki finansowe na dokonanie ataków	wysoki poziom umiejętności i wiedzy o ACS, średni poziom wiedzy o identyfikatorach i technologii IT średnie środki finansowe na dokonanie ataków	bardzo wysoki poziom umiejętności i wiedzy o ACS, wysoki poziom wiedzy o identyfikatorach i technologii IT duże środki finansowe na dokonanie ataków
Typowe przykłady	hotel	biura, małe przedsiębiorstwa	przemysł, administracja, obiekty finansowe	obszary wysoce wrażliwe (obiekty wojskowe, rządowe, R&D, obszary produkcji krytycznej)

* ACS (ang. *Access Control System*) – system kontroli dostępu (SKD) [przyp. aut.].



Rys. 3. Mur z cegły pełnej o grubości 25 cm, mierzonej bez tynku

Naszym zdaniem należy także przewidzieć zagrożenia pożarowe dla dokumentów i nośników. Można zaproponować również uproszczoną wersję:

4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych o istotnym znaczeniu dla prowadzonej działalności klasy S1, spełniające wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy wymagają wyższej klasy odporności szaf, ***a jeżeli na podstawie przeprowadzonego szacowania ich zastosowanie rodziłoby nieakceptowalne ryzyko dla przechowywanych dokumentów lub informatycznych nośników danych, związane z zagrożeniem pożarowym, odpowiednie szafy służące do przechowywania dokumentów lub do przechowywania informatycznych nośników danych, odporne na działanie ognia****.*

DRZWI ZEWNĘTRZNE I WEWNĘTRZNE

Tekst rozporządzenia proponowany przez PISA:

5) zewnętrzne drzwi wejściowe do pomieszczeń o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki ***i okucia*** *o klasie nie niższej niż klasa odporności* ***przywołana w normie dla danej klasy*** *drzwi;*

6) wewnętrzne drzwi do pomieszczeń o klasie odporności RC2 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki ***i okucia*** *o klasie nie niższej niż klasa odporności* ***przywołana w normie dla danej klasy drzwi*** […].

W tym miejscu należy wspomnieć, co tak naprawdę oznaczają klasy RC. W tabeli 2 pokazano niektóre parametry wytrzymałościowe i czasowe w zależności od klasy odporności.

OKNA, A WŁAŚCIWIE OTWORY OKIENNE

Tekst rozporządzenia proponowany przez PISA:

7) ***otwory okienne zabezpieczone w*** *klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia* […].

Przy tak zmodyfikowanym zapisie można stosować również inne zabezpieczenia mechaniczne, np. kraty lub rolety przeciwwłamaniowe, sklasyfikowane w klasie RC4.

ŚCIANY ZEWNĘTRZNE I WEWNĘTRZNE

Tekst rozporządzenia proponowany przez PISA:

8) ściany zewnętrzne ***z muru o grubości min. 250 mm, mierzonej bez tynku, wykonanego z pełnej cegły o wytrzymałości na ściskanie min. 15 MPa lub muru o grubości min. 150 mm, mierzonej bez tynku, wykonanego z betonu zbrojonego o wytrzymałości próbki sześciennej na ściskanie min. 15 MPa, lub muru o grubości min. 120 mm, mierzonej bez tynku, wykonanego z betonu zbrojonego o wytrzymałości próbki sześciennej na ściskanie min. 25 MPa albo innej konstrukcji o odporności na włamanie, adekwatnej do odporności drzwi klasy RC4****;*

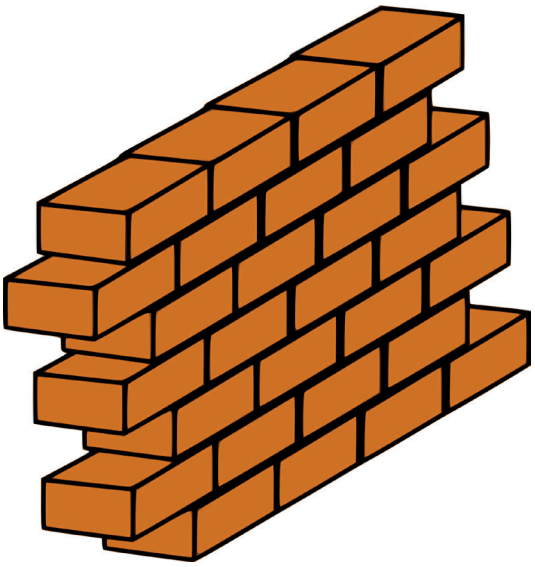
9) ściany wewnętrzne ***z muru o grubości min. 120 mm, mierzonej bez tynku, wykonanego z pełnej cegły o wytrzymałości na ściskanie min. 15 MPa lub muru o grubości min. 100 mm, mierzonej bez tynku, wykonanego z betonu zbrojonego o wytrzymałości próbki sześciennej na ściskanie min. 15 MPa, lub muru o grubości min. 80 mm, mierzonej bez tynku, wykonanego z betonu zbrojonego o wytrzymałości próbki***

Tabela 2. Wymagania dotyczące wytrzymałości zaczepów i zasuwek na obciążenie boczne zgodnie z PN-EN 12209 i PN-EN 1627 oraz minimalne czasy oporu

Klasa odporności RC	RC1N[1]	RC2N/RC2	RC3	RC4	RC5	RC6
Obciążenie boczne zasuwki, zaczepu	5 kN 510 kG	5 kN 510 kG	7 kN 714 kG	10 kN 1020 kG	10 kN 1020 kG	10 kN 1020 kG
Czas oporu	–	3 min	5 min	10 min	15 min	20 min

[1] Litera N oznacza, że w klasach RC1N i RC2N nie ma wymagań co do oszklenia.

Źródło: A. Tomczak: *Zamki elektromechaniczne. Niedoceniany standard zamknięć przejść w systemach kontroli dostępu i ewakuacji*. SEC&AS, nr 2/2019, s. 31.



Rys. 4. Mur z cegły pełnej o grubości 12 cm, mierzonej bez tynku

sześciennej na ściskanie min. 25 MPa albo innej konstrukcji o odporności na włamanie, adekwatnej do odporności drzwi klasy RC2.

W tekście rozporządzenia, w przypadku ścian zewnętrznych, przy dobrej intencji, do której zaraz wrócę, zastosowano nieprawidłowe odniesienie do wytrzymałości muru, a nie do klasy odporności drzwi – czego nie zapisano dla ścian wewnętrznych. Czyli w tekście rozporządzenia zapis dotyczący ścian wewnętrznych, odnoszący się *de facto* do klasy RC2, jest zapisem poprawnym, ale bardzo niekorzystnym, ponieważ wynika z niego, iż powinno się poddawać badaniom klasyfikacyjnym ściany wewnętrzne. Intencja autorów rozporządzenia, zawarta w opisie ścian zewnętrznych, szła w kierunku odciążenia operatorów od konieczności wykonywania badań klasyfikujących ściany zewnętrzne, ale zapisana w ten sposób i tak wymusza badanie ścian zewnętrznych w stosunku do enigmatycznej ściany z pełnej cegły. Dlatego nasza propozycja łączy ze sobą oba omówione wątki – odniesienie do klasy odporności ze wskazaniem, jakie mury spełniają te wymagania.

W przypadku określania grubości przykładowych ścian o odpornościach na włamanie adekwatnych do drzwi klasy RC2 i RC4 skorzystano z doświadczeń Instytutu Mechaniki Precyzyjnej, normy PN-EN 50518-1:2014-07 *Centrum monitoringu i odbioru alarmu. Część 1: Wymagania dotyczące rozmieszczenia i konstrukcji* oraz niemieckiego załącznika krajowego do normy DIN-EN 1627:2011-09 *Drzwi, okna, ściany osłonowe, kraty i żaluzje. Odporność na włamanie. Wymagania i klasyfikacja.* Na tej podstawie oraz biorąc pod uwagę stosowane w Polsce materiały budowlane, opracowano tabelę 3.

Trzeba również mieć świadomość, że wymagane odporności ścian, a co za tym idzie – także grubości murów mierzone bez tynków, nie są wygórowane. Dla porównania można przeanalizować zalecane grubości ścian konstrukcyjnych w budynkach. I tak, na pierwszej kondygnacji (parter) mur z cegły pełnej powinien mieć grubość 51 cm (2 cegły), na 1 i 2 piętrze – 38 cm (1,5 cegły), zaś powyżej – 25 cm (1 cegła), czyli tyle, ile jest wymagane dla klasy odporności drzwi RC4.

Tabela 3. Grubości murów, mierzone bez tynków, które pozwalają na założenie, że będą odpowiadały klasie odporności na włamanie zamontowanych w nich drzwi

Materiał \ Odporność	RC2	RC4
cegła pełna klasy 15 (K15)	120 mm	250 mm
żelbeton C12/15 (B15)	100 mm	150 mm
żelbeton C20/25 (B25)	80 mm	120 mm

PODSUMOWANIE

Z przedstawionej analizy wynika wniosek, iż do tworzenia skutecznych wymogów prawnych dla systemów zabezpieczeń konieczna jest dogłębna znajomości tematyki, która będzie opisywana w przepisach. Dlatego Polska Izba Systemów Alarmowych, wspomagana w swych działaniach przez pracowników Centrum Naukowo-Badawczego Ochrony Przeciwpożarowej, Instytutu Bezpieczeństwa Pożarowego NODEX, Instytutu Mechaniki Precyzyjnej oraz Instytutu Techniki Budowlanej, stara się działać na rzecz poprawności przepisów dotyczących zabezpieczeń technicznych i ich zgodności z normami technicznymi.

Na zakończenie uwaga dotycząca stosowania wymogów minimalnych w przepisach prawa. W przypadku tworzenia wymagań dla szerokiej grupy odbiorców zawsze może się zdarzyć, że znajdzie się jakiś wyjątkowy przypadek, w którym przepisy będą zbyt wymagające. Dlatego widoczny jest nacisk zainteresowanych środowisk na obniżanie wymagań minimalnych dla wszystkich, tak aby dopasować je do każdej możliwej sytuacji. Doświadczenia zagraniczne nie idą bynajmniej w tym kierunku. Na przykład niemiecki VDS stawia identyczne wymagania dla określonej grupy odbiorców, biorąc pod uwagę najbardziej typowe obiekty podlegające zabezpieczeniu. Jeżeli zdarzy się sytuacja, że ewidentnie wymogi te są zbyt wygórowane w konkretnym przypadku, istnieje możliwość wystąpienia o odstępstwo od postawionych wymagań, które musi być oczywiście odpowiednio umotywowane.

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym, redaktor naczelny SEC&AS