INTEGRACJA A STOPIEŃ ZABEZPIECZENIA SYSTEMU

Andrzej TOMCZAK

„Pytania z pozoru proste wymagają zawiłej odpowiedzi"
Zbigniew Herbert

Pytanie, które często przewija się w dyskusjach nt. integracji elektronicznych systemów zabezpieczeń (ESZ), dotyka istotnego tematu, dotyczącego tego, co stanie się ze stopniem zabezpieczenia danego systemu, po podłączeniu do innego systemu. Czyli należałoby zadać pytanie: jak integracja wpływa na stopnie zabezpieczenia poszczególnych ESZ?

Na początku należy stwierdzić, że zgodnie z aktualnie obowiązującymi normami na systemy alarmowe sygnalizacji włamania i napadu (SSWiN), systemy kontroli dostępu (SKD) oraz systemy dozoru wizyjnego (VSS, nazywane również CCTV), powyższe ESZ są klasyfikowane wg. tzw. stopni zabezpieczenia (ang. *grades*). Wyróżniamy cztery stopnie zabezpieczenia, od 1. do 4., z czego pierwszy jest najniższy, a czwarty najwyższy. Z praktyki wiadomo, że w systemach SWiN stopień 4. stosuje się wyjątkowo rzadko, natomiast w systemach kontroli dostępu i dozoru wizyjnego, wszystkie cztery stopnie mogą być bez problemu wykorzystywane. Czyli w systemach sygnalizacji włamania i napadu zazwyczaj stosuje się klasyfikację od stopnia 1. do 3., natomiast w pozostałych systemach pełne stopniowanie, od stopnia 1. do 4.

Źródła wiedzy

Zanim zagłębimy się w niuanse wpływu integracji na stopnie zabezpieczenia systemów, należy wskazać, skąd będziemy czerpać wiedzę na ten temat. Czytając art. 5.1. ustawy z dn. 7 lipca 1994 r. *Prawo budowlane* (Dz.U. 1994 Nr 89 poz. 414 z późn. zm.), możemy wywnioskować, że systemy zabezpieczeń należy projektować i budować w sposób określony w przepisach oraz zgodnie z zasadami wiedzy technicznej. Potoczny zwrot „zasady wiedzy technicznej", może być zakwalifikowany jako kontaminacja[1] frazeologiczna, polegająca na zmieszaniu dwóch wyrażeń „zasady sztuki" oraz „wiedza techniczna". Wykonywanie prac zgodnie z zasadami wiedzy technicznej można opisać jako wykonywanie prac zgodnie z:

- zasadami sztuki i dobrej praktyki, które są opisane np. w specyfikacjach technicznych oraz w przepisach prawa dotyczących wykonywania podobnych prac,
- aktualną wiedzą techniczną, której wymogi są określone m.in. w Polskich Normach.

Potwierdzają to zapisy rozporządzenia Rady Ministrów z dn. 29 maja 2012 r. *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych*, gdzie doprecyzowano, że elektroniczne systemy zabezpieczeń „należy wykonywać zgodnie z zasadami sztuki inżynierskiej i aktualnym poziomem wiedzy technicznej, opisanym w szczególności w odpowiednich Polskich Normach".

Systemy zabezpieczeń technicznych należy wykonywać:

- w sposób określony w przepisach,

- zgodnie z zasadami sztuki i dobrej praktyki, opisanymi np. w specyfikacjach technicznych oraz w przepisach prawa dotyczących wykonywania podobnych prac,

- zgodnie z aktualną wiedzą techniczną, opisaną m.in. w odpowiednich Polskich Normach.

Odpowiedzi na pytanie, dotyczące wpływu integracji na stopnie zabezpieczenia systemów, będziemy więc szukali w zasadach sztuki i dobrej praktyki, opisanych m.in. w rozporządzeniu MSWiA z dn. 7 września 2010 r. *w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne*, oraz w odpowiednich Polskich Normach i specyfikacjach technicznych.

Integracja wewnętrzna (natywna)

Integracja systemów zabezpieczeń może przebiegać na wiele sposobów. Może zostać np. zrealizowana na etapie produkcji. Taki system nazwiemy zintegrowanym wewnętrznie (natywnie) i będziemy traktować jako jeden system wielofunkcyjny. Tego typu integracja nie będzie wpływała na założony przez producenta stopień zabezpieczenia, chyba że taką zależność wytwórca wskaże. Innymi słowy, jeżeli wyprodukowano systemy sygnalizacji włamania i kontroli dostępu, zintegrowane natywnie, to realizacja poszczególnych systemów oddzielnie lub systemu zintegrowanego, oczywiście zgodnie z zaleceniami producenta, nie będzie miała wpływu na stopnie zabezpieczenia poszczególnych systemów. Tzn. jeżeli zintegrowano natywnie SSWiN w stopniu 3. oraz SKD w stopniu 4., to systemy te zainstalowane oddzielnie lub w wersji zintegrowanej zachowują wskazane przez producenta stopnie zabezpieczenia.

Integracja zewnętrzna bez ingerencji w integrowany system

Jeżeli zrealizujemy integrację, której celem będzie wyłącznie monitorowanie stanu klasyfikowanego systemu bez ingerencji w jego działanie, wówczas nie wpływamy na stopień zabezpieczenia monitorowanego systemu. Innymi słowy, pobieramy informacje z systemu, bez wpływania na ten system. Czyli dopóki system zewnętrzny nie ingeruje w system sygnalizacji włamania i napadu np. poprzez blokowanie czujek, uzbrajanie/rozbrajanie stref, potwierdzanie alarmów itp., integracja nie wpływa na stopień SSWiN. Podobnie, dopóki system zewnętrzny nie ingeruje w system kontroli dostępu, np. poprzez zdalne odblokowywanie przejść, integracja nie ma wpływu na stopień SKD.

Dopóki system zewnętrzny nie ingeruje w elektroniczny system zabezpieczeń np. poprzez blokowanie czujek, uzbrajanie/rozbrajanie stref, potwierdzanie alarmów, odblokowywanie przejść itp., integracja nie wpływa na stopień ESZ.

Aby „bezkarnie" realizować powyższe czynności należy wykorzystywać narzędzia dostarczane przez producenta w ramach sklasyfikowanego systemu, np. fabryczne interaktywne mapy synoptyczne.

Reasumując, trzymając się zasady nieingerowania w monitorowane systemy, można, bez wpływania na stopień systemu SWiN, czy też systemu KD, wykorzystywać dodatkowy zewnętrzny system monitorujący z mapami synoptycznymi, zrealizować integrację z systemem dozoru wizyjnego, czy też z systemem rejestracji czasu pracy (RCP).

Integracja zewnętrzna z ingerencją w integrowany system

Poprzednie sposoby integracji w sposób oczywisty nie wpływały na klasyfikację systemów, ponieważ nie miała miejsca nieprzewidziana w czasie klasyfikowania ingerencja zewnętrzna w system z poziomu innego systemu (system zintegrowany natywnie, traktowany jako jednolity

[1] Kontaminacja – skrzyżowanie i zespolenie elementów dwóch form, dwóch wyrazów lub dwóch połączeń wyrazowych [Słownik języka polskiego, PWN, 1978]

system wielofunkcyjny lub wyłącznie monitorowanie systemu). A co wtedy, gdy chcielibyśmy aby system zewnętrzny wpływał na działanie klasyfikowanego systemu?
Wówczas sprawa się komplikuje, ponieważ należy ustalić, czy na działania systemu zewnętrznego są przygotowane normy, czy też nie.

Integracja zewnętrzna z ingerencją w integrowany system, opisaną w normach

Taka sytuacja jest klarowna oraz dobrze opisana w normach i zasadach sztuki wykonywania systemów zabezpieczeń. Przytoczmy te zapisy za normą PN-EN 50131-1:2009 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 1: Wymagania systemowe* (w interpretacji autora tekstu angielski skrót I&HAS zastąpiono skrótem SSWiN):

„**6 Stopniowanie zabezpieczenia**
SSWiN powinien mieć określony stopień zabezpieczenia, który determinuje jego działanie. Stopień powinien być jednym z czterech stopni, gdzie stopień 1. jest stopniem najniższym, a stopień 4. stopniem najwyższym. Stopień SSWiN powinien być taki, jak jego część składowej najniższego stopnia. Gdy SSWiN jest podzielony na wyraźnie określone podsystemy, to SSWiN może zawierać w każdym podsystemie części składowe różnych stopni. Stopień podsystemu powinien być taki, jak stopień jego części składowej najniższego stopnia. Części składowe wykorzystywane wspólnie przez więcej niż jeden podsystem powinny mieć taki stopień, jak stopień podsystemu (np. urządzenia sterujące i obrazujące/systemy transmisji alarmu/sygnalizatory/zasilacze)".

Jeżeli system, realizujący zadania sterujące i obrazujące, ma ingerować w system sygnalizacji włamania i napadu, to zgodnie z powyższą zasadą, aby nie obniżyć stopnia zabezpieczenia, powinien być wykonany przynajmniej w identycznym stopniu, zgodnie z normą PN-EN 50131-3:2010 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 3: Urządzenia sterujące i obrazujące*. Ingerencja w system sygnalizacji włamania i napadu z poziomu systemu, realizującego zadania sterujące i obrazujące, o nieokreślonym stopniu zabezpieczenia, powoduje degradację systemu SWiN do poziomu systemu niesklasyfikowanego.

Obszar wymagań normatywnych, dotyczących administrowania systemem, może stwarzać kłopoty przy integracji np. zbieżność informacji o operatorach, wykonujących poszczególne operacje. Należy pamiętać o zachowaniu należytej staranności przy realizacji integracji, pamiętając o przepisach Załącznika 1 do rozporządzenia MSWiA z dn. 7 września 2010 r. *w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne*, które wskazują, aby elektroniczne systemy zabezpieczeń były wykonywane wg wymagań określonych w Polskich Normach, albo przynajmniej w sposób niesprzeczny z tymi wymaganiami, z czego wynika konieczność zadbania o to, aby w czasie integrowania brać pod uwagę zapisy odpowiednich norm.

Integracja zewnętrzna z ingerencją w integrowany system, nieopisaną w normach

Ta sytuacja znajduje odzwierciedlenie w specyfikacji technicznej PKN-CLC/TS 50131-7:2011 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Część 7: Wytyczne stosowania:*

„**7.3.1 Dobór elementów**
Zaleca się wybierać jedynie elementy spełniające wymagania dotyczące stopnia zabezpieczenia i klasy środowiskowej. (…) W przypadku gdy nie istnieją normy dotyczące danego elementu systemu, dopuszczalne jest użycie elementów nieposiadających stopnia ani klasy. W takich okolicznościach stopniem systemu będzie stopień zastosowanego elementu, o najniższym stopniu zabezpieczenia, podlegającego klasyfikacji".

Przytoczone już przepisy Załącznika 1 do rozporządzenia MSWiA z dn. 7 września 2010 r. wskazują, aby elektroniczne systemy zabezpieczeń były wykonywane wg wymagań określonych w Polskich Normach, albo przynajmniej w sposób niesprzeczny z tymi wymaganiami, z czego wynika konieczność zadbania o to, aby łącząc się z systemu nieobjętego zapisami norm, nie „uszkodzić" systemu o określonym stopniu zabezpieczenia, stosując się do zapisów normatywnych dla tego systemu.

Przykładami systemów nieobjętych Polskimi Normami są system przepustkowy oraz system obsługi gości. Przy zachowaniu „ostrożności" opisanej powyżej, podłączenie np. systemu obsługi gości do systemu kontroli dostępu nie obniży stopnia zabezpieczenia określonego dla SKD.

Podsumowanie

Przedstawiona powyżej analiza jest tylko pewnym przybliżeniem zrozumienia tego skomplikowanego problemu. W praktyce należy zwracać szczególną uwagę na tzw. „miękkie podbrzusze", wynikające z niekontrolowania integracji przez producenta, z reguły realizowanej na zamówienie i pod nadzorem odbiorcy systemu. Niestety często wiąże się to z naciskami na wykonanie integracji niezgodnie z wymogami opisanymi w normach.
Nie każdy system, wykorzystywany do realizacji integracji, został wyposażony w narzędzia zgodne z normami, przeznaczone do współpracy z innymi systemami. Ale z reguły do każdego systemu można „podłączyć" niekontrolowany „przycisk", który w sposób anonimowy zablokuje witalne funkcje.
Ale czy aby na pewno do tego powinniśmy dążyć?

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