DLACZEGO ZABEZPIECZENIA INSTALOWANE WEWNĄTRZ BUDYNKÓW NIE SĄ Z REGUŁY WYSTARCZAJĄCE?

Andrzej TOMCZAK

Rys. Sorhea

W większości osób pytanych o to, z czym im się kojarzą systemy alarmowe, najczęściej przychodzą na myśl różnego rodzaju czujki montowane w rogach chronionych pomieszczeń. Kiedy dowiadują się, że bardzo często montaż czujek w chronionych pomieszczeniach nie ma zasadniczego znaczenia dla bezpieczeństwa, nie mogą w to uwierzyć. A jednak…

WPROWADZENIE

Jeżeli przed nieprzygotowanym pracownikiem postawimy zadanie zorganizowania zabezpieczenia obiektu infrastruktury krytycznej czy nawet biura, efekt końcowy może nie gwarantować takiego poziomu ochrony, jakiego byśmy oczekiwali. Niestety w bardzo wielu przypadkach osiąga się tylko fałszywe poczucie bezpieczeństwa, które realia mogą brutalnie zweryfikować. A co dopiero ma powiedzieć osoba prywatna, która z reguły nie ma nic wspólnego z branżą zabezpieczeń? Gdy wprowadzamy się do nowego domu czy mieszkania, zwracamy często uwagę na uzyskanie poczucia bezpieczeństwa w tej nowej sytuacji życiowej. Ale właściwie powinniśmy zadać sobie trochę inne pytanie: czy wystarczy nam tylko poczucie bezpieczeństwa, czy chcielibyśmy być jednak skutecznie zabezpieczeni? Jak więc należy postąpić, aby nie tylko poczuć się bezpiecznie, ale faktycznie dobrze zabezpieczyć siebie i swoje mienie? Najprostsza prawidłowa odpowiedź to zlecić fachowcowi zaprojektowanie kompleksowego systemu zabezpieczeń, a następnie profesjonalnej firmie wykonanie tych zabezpieczeń. W naszej rzeczywistości pojawia się zwykle podstawowy problem – nie bardzo wiadomo, kto jest fachowcem godnym zaufania. I dotyczy to nie tylko systemów zabezpieczeń, ale również wielu usług związanych z budownictwem. W branży zabezpieczeń technicznych jeszcze jeden czynnik utrudnia podjęcie decyzji, a są nim ograniczone możliwości szybkiej weryfikacji kompetencji projektanta i instalatora systemu. Czujki bowiem mogą być estetycznie zamontowane, ale system zabezpieczeń źle zaprojektowany i wykonany. A to najczęściej zweryfikuje dopiero udana próba włamania czy napadu. Poniżej przedstawimy minimalny zakres wiedzy, jaką powinni dysponować z jednej strony dobrze wykształcony projektant i instalator systemów alarmowych sygnalizacji włamania i napadu, z drugiej strony świadomy inwestor tego typu systemów.

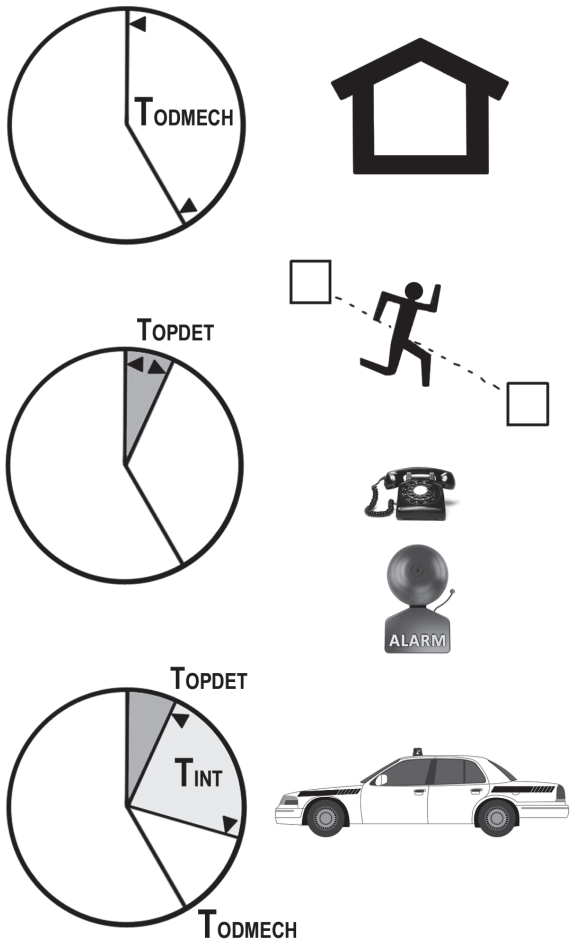
IDEA TWORZENIA SYSTEMÓW ZABEZPIECZEŃ

Podstawową zasadą prawidłowego zabezpieczania obiektów jest umiejętne powiązanie zabezpieczeń elektronicznych i mechanicznych z interwencją fizyczną. Interwencję może realizować agencja ochrony, policja czy np. zaprzyjaźnieni sąsiedzi. System elektroniczny powinien jak najszybciej wykrywać intruza,

Podstawową zasadą prawidłowego zabezpieczania obiektów jest umiejętne powiązanie zabezpieczeń elektronicznych i mechanicznych z interwencją fizyczną. System elektroniczny powinien jak najszybciej wykrywać intruza, a zabezpieczenia mechaniczne na tyle spowolnić jego działania, aby interweniujący dotarli na czas.

a zabezpieczenia mechaniczne na tyle spowolnić jego działania, aby pomoc dotarła na czas. Żaden z tych systemów, działając w oderwaniu od innych, nie może zagwarantować skutecznego zabezpieczenia. Trzeba pamiętać, że im wcześniej intruz zostanie wykryty, tym więcej mamy czasu na przeprowadzenie skutecznej interwencji. Należy tak zaprojektować system zabezpieczeń, aby na intruza – po wykryciu przez system alarmowy – czekały jeszcze przeszkody mechaniczne, spowalniające jego działanie. Jeżeli przy ocenie zabezpieczeń obiektów weźmie się powyższe pod uwagę, okaże się, że w naszym kraju bardzo wiele systemów alarmowych jest wykonywanych nieprawidłowo! Bo jeżeli system wykrywa intruza dopiero wewnątrz obiektu, to jest to sprzeczne z przedstawioną powyżej zasadą tworzenia systemów zabezpieczeń (ponieważ system alarmowy wykrywa intruza dopiero wtedy, gdy ten już pokonał zabezpieczenia mechaniczne).

Nie będzie truizmem stwierdzenie, że skuteczne zabezpieczenia opierają się na odwiecznej walce z czasem. Prawidłowo zaprojektowany system daje szansę zapobieżenia popełnieniu przestępstwa, a zaprojektowany nieprawidłowo – co najwyżej poinformuje o jego popełnieniu. Z punktu widzenia inwestora jest to szczególnie ważne, przede wszystkim od tego może zależeć wielkość poniesionych strat. Drobna różnica w interpretacji, ale skutki dla właściciela mogą być diametralnie różne. Tę ideę można przedstawić na schemacie czasowym, opartym na idei stopera (rys. 1), który powstał na podstawie grafiki opublikowanej w 1993 r. w materiałach szkoleniowych firm



T_{ODMECH} – czas odporności mechanicznej to czas potrzebny na pokonanie najsłabszego zabezpieczenia mechanicznego, umożliwiającego wtargnięcie do chronionego obiektu.

T_{OPDET} – czas opóźnienia detekcji to czas od rozpoczęcia ataku do momentu wykrycia intruza przez elektroniczny system zabezpieczeń oraz powiadomienia interweniujących i/lub włączenia sygnalizacji akustycznej.

Uwaga: Uruchamianie sygnalizacji dźwiękowej nie jest obligatoryjne.

T_{INT} – czas interwencji to czas od momentu dostarczenia informacji do centrum odbiorczego alarmów do momentu rozpoczęcia interwencji na miejscu zdarzenia.

System zabezpieczeń został prawidłowo zaprojektowany i wykonany, jeżeli:

$$T_{ODMECH} > T_{OPDET} + T_{INT}$$

Rys. 1. Schematy czasowe obrazujące graficznie ideę właściwego zabezpieczenia systemem SwiN

Źródło: Opracowanie własne, na podst. materiałów firmy Siemens

Alarmcom i Cerberus (wykupionych na początku XXI w. przez firmę Siemens). Atak intruza dzieli się na trzy – współbieżne lub nie – fazy, których układ będzie informacją, czy system zabezpieczeń został wykonany zgodnie z zasadami sztuki.

PODSUMOWANIE

Po zapoznaniu się znaną od dawna regułą tworzenia systemów zabezpieczeń należy zadać pytanie: „Dlaczego tak często systemy zabezpieczeń wykonywane są nieprawidłowo?”. Dla fachowca odpowiedź jest oczywista, acz złożona.

Ochrona obrysowa

Ochrona peryferyjna

Ochrona obwodowa

Rys. 2. Przykłady metod wczesnego wykrywania potencjalnego intruza

Źródło: Sorhea

Po pierwsze, wykonywanie zabezpieczeń wewnątrz obiektów jest prostsze i tańsze niż zrealizowanie ochrony: obrysowej, peryferyjnej czy obwodowej (która bardzo często wymusza instalowanie urządzeń w warunkach zewnętrznych). Wystarczy trochę przewodów, kilka czujek, centrala, sygnalizatory i... najczęściej powstaje twór wyglądający jak elektroniczny system zabezpieczeń, ale w najlepszym przypadku niebędący systemem zabezpieczającym, a tylko informującym o popełnionym przestępstwie. Przypomina to popularne rozwiązania oferowane na naszym rynku, które można obrazowo opisać tak: jesteś na plaży, zobacz na ekranie komórki, jak okradają twój dom. Na rys. 2 przedstawiono przykłady sposobów zabezpieczenia obiektu, realizowane na zewnątrz budynku, które dobrze wpisują się w hasło wczesnego wykrywania intruza[1].

Po drugie, wielu pracujących w branży nie zostało prawidłowo przeszkolonych (albo w ogóle nie przeszli szkoleń), mogą więc popełniać nawet podstawowe błędy. Nie od dziś wiadomo, że dziedzina projektowania i instalowania systemów zabezpieczeń jest w Polsce traktowana po macoszemu. Niezależni branżowi projektanci i instalatorzy są „wyjęci” spod prawa budowlanego i często zastępowani przez projektantów branży elektrycznej i wykonawców instalacji elektrycznych. Ci, mimo że są dobrze w prawie budowlanym umocowani, nie mają z reguły podstawowej wiedzy o zasadach sztuki projektowania i instalowania zabezpieczeń elektronicznych. Co gorsza, najczęściej nawet nie zdają sobie z tego sprawy.

Dlatego w czasopiśmie SEC&AS zajmujemy się edukacją osób zainteresowanych, m.in. pokazując, jak należy prawidłowo zabezpieczać obiekty. W tym numerze koncentrujemy się na wczesnym wykrywaniu, a także na spowolnieniu ataku potencjalnego intruza.

[1] Więcej szczegółów na temat tworzenia stref zabezpieczeń obiektów można znaleźć w artykule tegoż autora *Podstawy zabezpieczania obiektów infrastruktury krytycznej* – SEC&AS 1/2017 str. 66

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym