OCHRONA OBIEKTÓW ROZPROSZONYCH, O RÓŻNYM PRZEZNACZENIU NA PRZYKŁADZIE OBIEKTÓW ENERGETYKI ZAWODOWEJ

Czas pandemii zmienił trendy w wielu branżach, także w ochronie obiektów. Reżim sanitarny, ograniczył do minimum kontakt z osobami, często związany ze stosowaniem dodatkowych urządzeń do pomiaru temperatury, dezynfekcji, utrudnił procedury ochronne. W wielu przypadkach łatwiejsze okazało się ograniczenie służb ochrony, a w zamian zastosowanie zabezpieczeń elektronicznych. Znacząco przyspieszyły rozwiązania z systemami dozoru wizyjnego, z funkcją „asysty" zdalnego operatora z centrum dozoru, w którą to obsługę wyposażane są centra monitorowania alarmów. Takie rozwiązanie sprawdza się, jeżeli prawidłowo wykonano analizę ryzyka, zgodności z obowiązującymi przepisami i skutecznie określono oczekiwania klienta i obowiązki usługodawcy w umowach. Niestety, zdarzają się sytuacje, kiedy zastosowane rozwiązanie ocenianie jest wyłącznie na podstawie chwilowej skuteczności odsunięcia problemu w czasie, bez szacowania jego ewentualnych skutków w przyszłości.

Usługa zdalnej ochrony, portiera czy asysty w obiekcie staje się coraz popularniejsza. Zdalny operator wykorzystując system dozoru wizyjnego wraz ze zintegrowanymi systemami alarmowymi, łącznością telefoniczną lub systemami głośników rozmieszczonych w obiekcie. Zdalnie nadzoruje i asystuje pracownika podczas wykonywania zadań np. samotnego strażnika, wpuszczając kierowcę, pierwszego pracownika pojawiającego się w pracy lub ostatniego opuszczającego obiekt. Podobnie funkcjonują rozwiązania w dużych obiektach, szczególnie infrastruktury krytycznej (IK). Jako przykład

Zdj. 1. Pożar transformatora wysokiego napięcia w stacji GPZ
Źródło: https://ise.pl/forum/zdjecia-i-filmy/pozar-gpz-pod-plockiem-10633

opisane zostaną rozwiązania w obiektach energetyki zawodowej. Poza ochranianą bezpośrednią wartością mienia pojawia się dodatkowy, znacznie bardziej istotny czynnik, którym jest wymóg zachowania ciągłości działania – dostaw energii. Obiekty energetyki podlegające ochronie to budynki biurowe, magazyny warsztaty, serwerownie, dyspozytornie, obiekty sieci energetycznej, stacje transformatorowe, linie energetyczne, główne punkty zasilania (GPZ) czy mienie ruchome. Sposób zróżnicowanej, ale jednocześnie zintegrowanej ochrony opisany został poniżej.

Przystępując do ochrony pojedynczego obiektu i dokonując analizy ryzyka napotyka się wiele trudności od warunków usytuowania, funkcji obiektu, architektury, dostępu osób postronnych, ruchu osobowego i pojazdów itp. Skuteczne zarządzanie bezpieczeństwem pozwala na ich przezwyciężenie, także w przypadku wielu różnych obiektów, usytuowanych w odrębnych lokalizacjach. Tak jest z rozproszonymi obiektami energetyki zawodowej. Występuje wzajemna zależność oraz podział funkcjonalny i zadaniowy infrastruktury na Polskie Sieci Energetyczne, Operatorów, Dystrybucję i Wytwarzanie energii elektrycznej. Podstawowe zagrożenia związane z ochroną obiektów związane są z utratą, uszkodzeniem mienia oraz przerwaniem dostaw energii. Co ciekawe, do wspomnianych zagrożeń może dojść w wyniku różnych czynników od warunków atmosferycznych, przez włamania i kradzieże, po sabotaż, atak terrorystyczny, czy włamanie do infrastruktury teletechnicznej. Skutki pandemii covid podniosły znaczenie czynnika biologicznego w rankingu zagrożeń, wymuszając reorganizację sposobu ochrony obiektów. Pulę uzupełniają także pożary[1] niszczące linie energetyczne i stacje, ale nie tylko. Jedno z ciekawszych zdarzeń dotyczyło nowo wybudowanej linii średniego napięcia, ze zbrojonymi słupami wibrobetonowymi, uszkodzonej przez… bobry. Doprowadziły one do przewrócenia drzew na linię energetyczną, co spowodowało skręcenie i popękanie słupów, a w konsekwencji długą przerwę w dostawach energii[2]. W mediach pojawiają się informacje o przypadkach wtargnięcia osób nieuprawnionych na teren elektrowni, czy obserwowane nad obiektami IK drony. Takich przykładów zagrożeń bezpieczeństwa obiektów energetyki zawodowej związanych z utratą mienia lub przerwaniem dostaw energii można wymieniać wiele i pojawiają się nowe. Istotą jest jednak efektywne eliminowanie zagrożeń

[1] https://wpolityce.pl/spoleczenstwo/286600-pozar-linii-wysokiego-napiecia-skala-zniszczen-jest-gigantyczna

[2] https://nto.pl/miec-bobra-za-sasiada/ar/3954365

GEMOS
advanced PSIM

Od 28 lat integrujemy systemy i aplikacje bezpieczeństwa w obiektach

www.ela.pl

www.facebook.com/BuildingManagementSystems

linkedin.com/company/elacompil

i minimalizowanie występujących skutków. Główną rolę odgrywa tutaj analiza ryzyka i zdarzeń w długim okresie. Ponieważ infrastruktura IK wymaga zarządzania ciągłością działania, na bieżąco należy aktualizować potrzeby i procedury ochronne. Rzetelna analiza zdarzeń może doprowadzić do zaskakujących wniosków, odnośnie przewidywanych zagrożeń np. dotyczących ryzyka włamania do stacji GPZ i rzeczywistych ich skutków. Bezpośrednio wpływa to na wybór sposobu ochrony, stosowanych urządzeń detekcyjnych czy procedur. Obiekty energetyki zawodowej od lat wyposażane są w nowoczesne technologie bezpieczeństwa. Systemy alarmowe z różnych, rozproszonych obiektów zintegrowane są i nadzorowane przez redundantne stanowiska monitorowania alarmów. Stanowiska wyposażone w system integrujący kategorii PSIM (ang. Phisical Security Information Management) pozwalają na wszechstronne dopasowanie zarządzania bezpieczeństwem obiektów do potrzeb i hierarchicznej struktury energetyki zawodowej. Systemy kategorii PSIM służą do zarządzania obiektami nie tylko w zakresie integrowania systemów alarmowych i prowadzenia ewakuacji. Pozwalają zarządzać dostępem do obiektów, ruchem osób i pojazdów, eksploatacją systemów i urządzeń, nadzorować infrastrukturę teleinformatyczną i automatykę budynkową, śledzić lecące drony, generować raporty, rozliczać pracę użytkowników oraz operatorów i wiele innych. W zależności od potrzeb pozwalają ingerować operatorom w zaprogramowane procedury i podejmować decyzje (wymagane większe kompetencje operatorów) lub generują wstępnie zweryfikowane alarmy oraz wyświetlają zaprogramowane procedury, które operatorzy wykonują zgodnie z przyznanymi uprawnieniami[3]. Obsługa takich stanowisk może być realizowana przez spółkę wchodzącą w skład grupy energetycznej, lub poprzez usługę firmy zewnętrznej. Jednym z najbardziej efektywnych modeli ochrony obiektów energetyki zawodowej jest ten, w którym za eksploatacje systemów zabezpieczeń elektronicznych i operatorów tych systemów, odpowiada wyodrębniony podmiot np. z grupy spółek energetycznych. Odpowiedzialne są one wtedy za eksploatację systemów zabezpieczeń elektronicznych i stanowiska operatorów monitorowania alarmów. Odrębną usługą ochrony są

[3] C.Mecwaldowski, „Zarządzanie rozproszoną infrastrukturą krytyczną na przykładzie obiektów służby więziennej" A&S 5/2019,

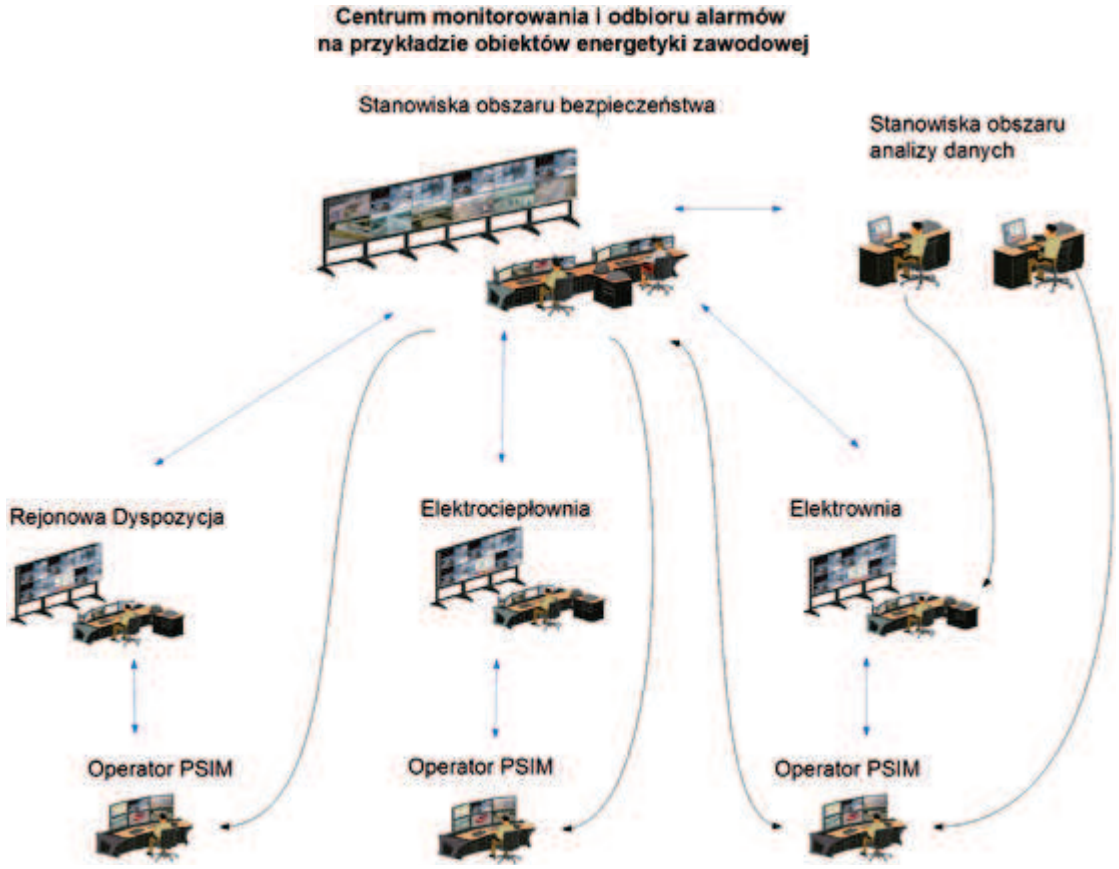
Zdj. 2. Ćwiczenia antyterrorystyczne w elektrowni Dolna Odra
Źródło: https://ono24.info/atak-terrorystyczny-w-elektrowni-dolna-odra-zdjecia,a8583

grupy interwencyjne, reagujące na powiadomienia ze wspomnianych stanowisk monitorowania alarmów. W zależności od liczby ochranianych obiektów, ich rangi w strukturze zachowania ciągłości dostaw energii, tworzona jest odpowiednia liczba stanowisk operatorów i centra monitorowania alarmów. Każde takie stanowisko powinno być obsługiwane przez minimum dwóch operatorów, wyposażonych w środki łączności. W przypadku wystąpienia alarmu z obiektu, następuje wstępna weryfikacja zdarzania i reakcja np. wezwanie grupy interwencyjnej, straży pożarnej itp. Istotnym narzędziem weryfikacji alarmów jest tutaj system dozoru wizyjnego, który w obiektach typu stacja GPZ pełni dodatkową, niezależną funkcję dla dyspozytorów mocy, pozwalając na wgląd w procesy przełączeniowe urządzeń energetycznych. Co jednak należy podkreślić, nie wolno łączyć funkcjonalnie w jednym, stanowiska dyspozytora mocy i operatora zintegrowanych systemów alarmowych.

Grupy interwencyjne mogą być zupełnie niezależnym podmiotem i świadczyć usługi na rzecz obiektów energetyki zawodowej. Takie firmy podejmując się ochrony IK powinny być weryfikowane i nadzorowane przez służby bezpieczeństwa państwa. Dotyczy to nie tylko wpisu na listę kwalifikowanych pracowników ochrony, szeregu licencji i poświadczenia bezpieczeństwa przemysłowego. Niedopuszczalna jest sytuacja, w której mogłoby dojść do zmian, zastępstw kadry ochrony osobami nieposiadających kwalifikacji i kompetencji w zakresie ochrony infrastruktury krytycznej.

Kolejne istotne zagadnienie związane z trudnością ochrony obiektów energetyki zawodowej to specyfika funkcjonalna obiektu. Sieciami energetycznymi 24/7/365 zarządzają dyspozytorzy. Obowiązują ścisłe dokumentowane i nadzorowane procedury bezpieczeństwa pracy przy urządzeniach energetycznych. Nikt nie może wejść do stacji transformatorowej bez nadzoru osoby dopuszczającej. Mimo wystąpienia zagrożenia, nie zawsze możliwe jest wejście służb ochrony do obiektu lub na jego teren. Nawet w przypadku włamania, służby ochrony nie zostaną dopuszczone do wejścia w obszar urządzeń średniego lub wysokiego napięcia. Tu działania służb ochrony muszą być dedykowane, a procedury różnią się od stosowanych w innych obiektach. Niewiedza i wejście na teren takich obiektów w sytuacji zdarzenia np. włamania, stanowi zagrożenie życia dla służby ochrony. Należy stawiać wyższe wymagania kompetencyjne wobec służb ochrony infrastruktury krytycznej. To także egzekwowanie większej wiedzy na temat obiektów i występujących zagrożeń związanych z ich funkcjonowaniem, przeprowadzania cyklicznych szkoleń oraz ćwiczeń współdziałania. Takie ścisłe przestrzegane procedur dopuszczania do pracy przy urządzeniach energetycznych, pozwala na ograniczone do minimum stosowanie systemów kontroli dostępu (np. w stacjach rozdzielczych, transformatorowych czy GPZ). Jednocześnie niezbędne są systemy telewizji dozorowej służące operatorom do weryfikowania alarmów, a wyposażane w inteligentną analizę sygnału wizyjnego także, jako źródło alarmowania. Systemy dozoru wizyjnego pozwalają niezależnie dyspozytorowi na wgląd w pracę urządzeń stacji wysokiego napięcia, stan linii lub dozór pracy techników. Inny niezbędny system alarmowy to system sygnalizacji pożaru, nie tylko w obiektach biurowych, magazynowych, warsztatach, ale także w stacjach energetycznych. W przestrzeniach otwartych, obszarach linii energetycznych, możliwe jest stosowanie kamer termowizyjnych oraz inteligentnej analizy obrazu dokonującej detekcji ognia i dymu.

Zdj. 3. Aktywiści Greenpeace protest na kominie chłodni elektrowni Bełchatów
Źródło: \Greenpeace\Internet



Zdj. 4. Przykładowa hierarchiczna struktura stanowisk operatorów PSIM
Źródło: opracowanie własne na podstawie Winsted

Odrębnym zagadnieniem ochrony obiektów IK jest cyberbezpieczeństwo, którego rola jest równie ważna jak ochrona fizyczna. Analiza ryzyka wymaga uwzględnienia wszelkich podatności od bezpośredniego dostępu do urządzeń infrastruktury IT, po łącza telekomunikacyjne i ryzyko zdalnego włamania. Niezwykle istotne jest czy obiekty posiadają własną infrastrukturę telekomunikacyjną, czy korzystają z usług innych dostawców i jakie gwarancje cyberbezpieczeństwa daje operator usług kluczowych. Aby przerwać dostawy energii nie trzeba uszkadzać transformatora lub innych elementów sieci energetycznej. Do osiągnięcia celu wystarczy włamanie do sieci teleinformatycznej sterującej automatyką sieci energetycznej. Takie przypadki miały już wielokrotnie miejsce na świecie (także w Polsce), a możliwości powstania zagrożenia jest wiele. Prostym przykładem mogą być rozrzucone na terenie pamięci pendrive z oprogramowaniem lub mini routerem bezprzewodowym. Nieświadomy zagrożeń znalazca-pracownik, podłączając takie urządzenie do aktywnego portu USB komputera, drukarki w biurze, może nawet nie zauważyć, co dzieje się w tle systemu (np. zobaczy nieszkodliwe pliki, które jednak skłonią go do dłuższego przeglądania zawartości, dając tym samym czas przestępcy na zdalną penetrację systemów). Innym słabym punktem bezpieczeństwa są technologie sieci Wi-Fi czy GSM. Bezpieczeństwa nie gwarantuje także lokalna sieć Wi-Fi nie wychodząca zasięgiem poza granice chronionego obiektu, możliwy jest zdalny dostęp np. przy użyciu drona. Nie wystarczy wprowadzić zakazu stosowania Wi-Fi, obiekty mogą zostać nieświadomie wyposażone w urządzenia, które coraz częściej taką funkcje mają wbudowaną np. przy okresowych zakupach i wymianie sprzętu drukarek, monitorów, telewizorów, projektorów, czytniki kodów kreskowych, terminali podpisu cyfrowego, coraz powszechniej stosowanych urządzeń IoT i innych.

Przywołane do dyskusji, zagadnienia ochrony obiektów energetyki zawodowej, mają na celu przybliżenie czytelnikowi skali trudności i wyzwań, z jakimi musi się zmierzyć służba ochrony. Profesjonalna ochrona rozległych obiektów, o różnym przeznaczeniu, pozostających w dyspozycji różnych podmiotów, rozproszonych po terenie kraju jest możliwa, poprzez:

- wdrożenie systemu zarządzania ciągłością działania,
- bieżące, rzetelne prowadzenie analizy ryzyka, audytów bezpieczeństwa,
- stosowanie nowoczesnych urządzeń i systemów zabezpieczeń elektronicznych, zintegrowanych systemem kategorii PSIM, hierarchiczną i redundantną strukturą, kompetentnymi operatorami współpracującymi z grupami interwencyjnymi,
- utrzymywanie maksymalnie wysokiego poziomu cyberbezpieczeństwa.

kpt. mgr inż. Cezary Mecwaldowski
Wykładowca zakładu szkolenia ochronnego w Centralnym Ośrodku Szkolenia Służby Więziennej w Kulach.