ZASADY OCENY ZAGROŻEŃ DLA BEZPIECZEŃSTWA INSTALACJI PRZEMYSŁOWYCH W WYNIKU NIEPOŻĄDANYCH DZIAŁAŃ STRON TRZECICH

Mieczysław Borysiewicz
Centrum Doskonałości MANHAZ, Instytut Energii Atomowej - Świerk

W wielu krajach po 11. września 2001 r. zintensyfikowano prace nad podniesieniem poziomów bezpieczeństwa instalacji przemysłowych i ważnych infrastruktur krajowych w odniesieniu do potencjalnych aktów terroru i sabotażu. Systematyczne zwiększanie bezpieczeństwa jest uwarunkowane wieloma czynnikami, główne z nich to: rodzaj zagrożenia, stopień podatności różnych elementów przemysłowych na poszczególne działania niepożądane, możliwe skutki zdarzeń, awarii czy ataków, a także „atrakcyjność" niektórych elementów infrastruktury (najbardziej strategicznych) dla stron trzecich. W przypadku zagrożenia terrorystycznego, punktami krytycznymi – najbardziej narażonymi na atak, są elementy strategiczne dla całej instalacji, a zwłaszcza takie, których awaria spowoduje zatrzymanie pracy znacznej części instalacji oraz elementy, których awaria spowoduje bardzo duże skutki dla środowiska i pobliskiej ludności.

Kluczowym elementem dla osiągnięcia celu jest przeprowadzenie analiz podatności SVA (Security Vulnerability Analysis) i wykorzystanie jej wyników do sporządzania planu bezpieczeństwa instalacji w aspekcie zapobiegania niepożądanym działaniom i minimalizowania ich skutków. Jest to proces analityczny, w którym wyznacza się typy i warunki dla potencjalnych zagrożeń terrorystycznych i sabotażowych, prawdopodobieństwa skutków oraz możliwe następstwa. Najbardziej znane metody ocen ryzyka i podatności na atak to: metoda SVA opracowana przez Center for Chemical Process Safety (CCPS), metody równoległe przygotowane przez ExxonMobil Chemical, BASF, Air Products, Georgia Pacific oraz metoda VAM-CF opracowana przez Sandia National Laboratory w USA. Powyższe metodologie opierają się na kilku wspólnych i niezbędnych krokach: zidentyfikowanie celów i opracowanie planu analiz podatności, charakterystyka potencjalnych miejsc zagrożonych, identyfikowanie zagrożeń, analizy podatności, określenie środków zaradczych. W poniższej pracy przedstawiono metodę analizy i zarządzania bezpieczeństwem SVA rekomendowaną przez CCPS.

1. PODSTAWOWE ELEMENTY ANALIZ SVA

1.1. Definicja pojęć stosowanych w metodzie SVA

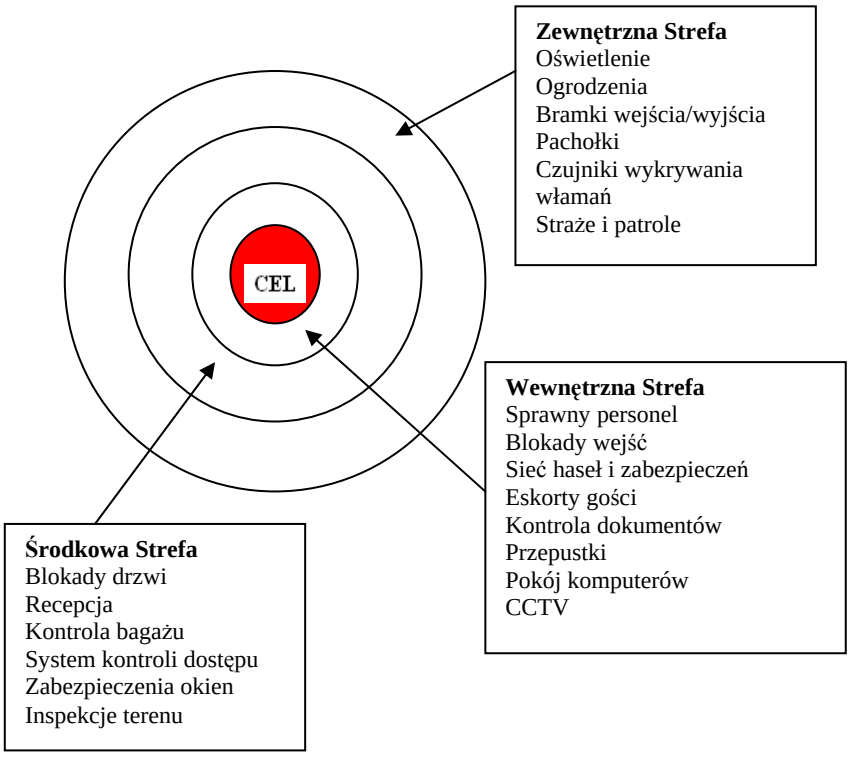
SVA (Security Vulnerability Analysis) jest procesem określającym prawdopodobieństwo wystąpienia niepożądanego zdarzenia, opartym na analizie podatności oraz szacującym zasięg skutków. SVA wykorzystuje w celu określenia stanu bezpieczeństwa danej instalacji stacjonarnej głównie analizy jakościowe. Wynikiem analiz jest uzyskanie listy rankingowej celów najbardziej zagrożonych atakiem ze strony terrorystów, na podstawie której podejmowane są decyzje o środkach zaradczych. Oszacowanie podatności danego celu na atak jest zadaniem trudnym, gdyż jest to obiektywny proces oszacowywania subiektywnych osiągów ekspertów.

Skutki rozpatrywane w SVA mogą się różnić wielkością i charakterem i zakresem od skutków rozważanych w standardowych analizach ryzyka poważnych awarii. W analizach przyjmuje się z reguły, ze terrorysta chce zmaksymalizować szkodę i zaatakować cel, który jest dość łatwo dostępny.

Skutki niepożądanego działania rozważa się w kilku kategoriach: wpływ na zdrowie ludzkie, straty finansowe, negatywne oddziaływanie na środowisko zewnętrzne.

W ramach SVA **zagrożenie** jest definiowane jako okoliczność, mogąca spowodować utratę lub zniszczenie dóbr materialnych i/lub straty w ludziach i w środowisku. Może być zdefiniowane jako zamiar lub zdolność terrorysty do przedsięwzięcia działań powodujących szkody w danym zakładzie, szkody dla środowiska i zdrowia ludzkiego. Źródłem zagrożenia może być: inny rząd, niezadowolony pracownik albo kontrahent, kryminalista, gwałtowny aktywista, terrorysta (polityczny, religijny, środowiskowy).

Podatność jest zdefiniowana jako słabe rozwiązania inżynieryjno-organizacyjne, które mogą być wykorzystane przez strony trzecie dla wyrządzenia szkód. Podatność na atak może wynikać z rodzaju prowadzonej działalności, ze złej polityki zarządzania zakładem, z niewłaściwego zabezpieczenia obiektów, czy też z innych czynników operacyjnych.



Rys. 1. Fizyczne i cybernetyczne strefy i pierścienie ochronne.

Atrakcyjność celu może wynikać z wielkości i rodzaju szkody jaka może spowodować jego zaatakowanie. Nie wszystkie cele są jednakowo atrakcyjne dla terrorysty, co ma znaczący wpływ na określenie prawdopodobieństwa ataku na dany obiekt.

Środki zaradcze są działaniami podjętymi w celu zmniejszenia albo wyeliminowania jednej albo więcej cech słabych instalacji. Środki zaradcze obejmują sprzęt komputerowy, systemy techniczne,

oprogramowanie, procedury i kontrole administracyjne. Podczas analiz SVA środki zaradcze wybiera się na podstawie oceny ich dostępności, efektywności działania, niezawodności. Do środków zaradczych można zaliczyć: bezpieczeństwo fizyczne, kontrolę dostępu, zapobieganie stratom, zarządzanie inwentarzem chemikaliów, zarządzanie w sytuacjach kryzysowych i awaryjnych, politykę bezpieczeństwa w tym procedury postępowania, bezpieczeństwo sieciowe i bezpieczeństwo danych. Redukcja ryzyka działań terrorystycznych może być prowadzona poprzez zapobieganie, detekcję i opóźnianie działań terrorysty (DDD - Deter, Detect and Delay), tworzenie fizycznych i cybernetycznych stref i pierścieni ochronnych (Rys.1), odpowiednią praktykę i procedury, czy też stosowanie systemów i technologii naturalnie bezpiecznych.

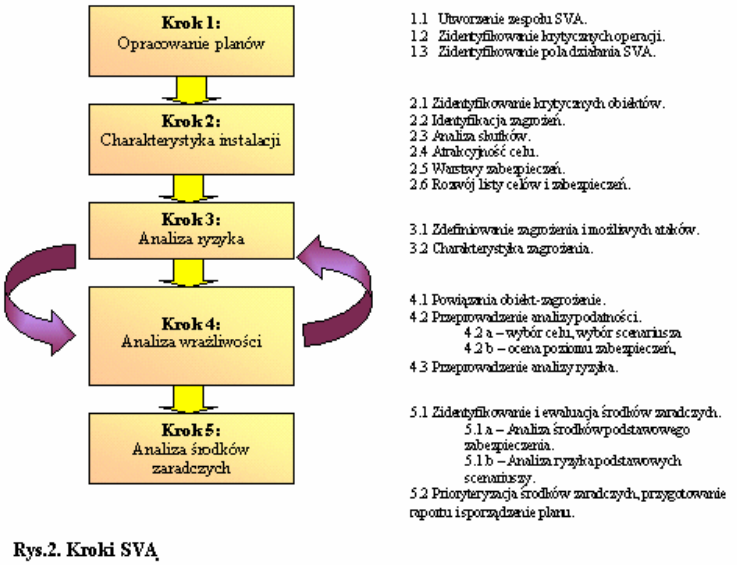
2. WYMAGANE KROKI SVA

Wymagane kroki przeprowadzenia SVA zgodnie z metodyką opracowaną przez Centre of Chemical Process Safety przedstawia rys. 2 . Poniżej są one omówione bardziej szczegółowo.

Krok 1: Planowanie procesu SVA:

Planowanie SVA wymaga określenia celów i zakresu analiz. Najważniejsza w tym kroku jest identyfikacja krytycznych operacji i zakresu działań. Ważny jest również wybór i utworzenie zespołu SVA.

Uważne spełnienie wymagań SVA wymaga dokładnego i kompletnego planowania działań. Najważniejsze w tym kroku jest identyfikacja krytycznych operacji i pola działania. Ważne jest również wybór i utworzenie zespołu SVA.



Rys.2. Kroki SVA

Rys. 2. Kolejne kroki analizy podatności SVA.

Określenie celów analizy SVA

Konieczne jest: zidentyfikowanie źródeł zagrożeń bezpieczeństwa, przeprowadzenie analiz podatności instalacji produkujących, przetwarzających, przeładowujących lub magazynujących materiały niebezpieczne i dokonanie oceny środków zaradczych stosowanych do ochrony publicznej, pracowników, interesów państwowych, środowiska przyrodniczego i samego zakładu.

Zidentyfikowanie obszaru analiz SVA

Należy opracować najpierw plan określający priorytety analiz obiektów i potencjalnych celów ataku. Należy przy tym uwzględnić cztery podstawowe grupy zdarzeń:

- utrata szczelności powłok zewnętrznych urządzeń i sprzętu zawierających niebezpieczne substancje, w wyniku działań umyślnych,
- kradzież lub niewłaściwe użycie niebezpiecznych materiałów (np. substancji chemicznych) z zamiarem wyrządzenia szkód w zakładzie lub poza zakładem,
- zanieczyszczenie lub popsucie produktów wytwarzanych w zakładach z zamiarem spowodowania ofiar, zranień i chorób pracowników i wśród społeczeństwie,
- degradacja zasobów, infrastruktury lub funkcji biznesowych zakładu i /lub całej branży/.

System prioryteryzacji powinien szeregować substancje chemiczne jako bardzo, średnio i mało niebezpieczne, biorąc pod uwagę ich własności chemiczne, możliwość użycia ich jako broni chemicznej, czy broni masowego rażenia. Materiały chemiczne, sklasyfikowane jako bardzo niebezpieczne, powinny w pierwszej kolejności być zabezpieczane, ze względu właśnie na ich dużą podatność i wrażliwość.

Analiza SVA powinna być skoncentrowana na całym zakładzie, wszystkich jej elementach i operacjach krytycznych, a tam gdzie to ma zastosowanie, również na obiektach sąsiadujących, nie należących do zakładu.

Krok 2: Charakterystyka instalacji:

Krok ten obejmuje charakterystykę elementów najbardziej podatnych na zagrożenie w tym: potencjalne cele ataku, ich lokalizację i „terrorystyczną atrakcyjnych", detale rozwiązań technicznych, identyfikację zagrożeń, oszacowanie skutków potencjalnych ataków oraz listę celów i zabezpieczeń. Krok ten obejmuje też ocenę środków zaradczych podejmowanych w razie zaistnienia ataku terrorystycznego. Po zidentyfikowaniu zabezpieczeń i określeniu atrakcyjności celów ustala się harmonogram istniejących modyfikacji lub wprowadzenia dodatkowych środków prewencji i wspomagania reagowania w sytuacji zaistnienia ataku.

Identyfikowanie obiektów krytycznych

Zwraca się uwagę głównie na obiekty zawierające i przetwarzające niebezpieczne materiały chemiczne oraz na sposoby zabezpieczeń tych obiektów (systemy fizyczne i systemy automatyki zabezpieczeniowej. Systemy sterowania procesem i automatyki zabezpieczeniowej mogą być zagrożone fizycznym lub cybernetycznym atakiem z zewnątrz. Krytyczne zasoby zabezpieczenia dotyczą m.in.: procesów chemicznych, przechowywania, przetwarzania, transportu; zbiorników magazynujących; rurociągów wewnętrznych; surowców systemów sterowania; personelu operacyjnego; produktów końcowych; systemów pomocniczych (zaopatrzenia w energię elektryczną; wodę; gaz); systemu telekomunikacyjnego; przerobu odpadów; informacji biznesowych; komputerowego systemu zarządzania biznesowego; powiązań w zakładzie oraz kontaktów z klientami.

Identyfikacja zagrożeń

Krok identyfikacji zagrożeń jest procesem identyfikowania i zrozumienia jak zabezpieczenia krytyczne wpływają na możliwe zajścia i wypadki, i jak wówczas zmienia się poziom zagrożenia. Podatność na zagrożenie powinna być określana na podstawie poniższych informacji:

- Lista niebezpiecznych chemicznych substancji oraz ich lokalizacja, koncentracja, ilość i stan substancji chemicznych obecnych w zakładzie/ instalacji itp. Zespół SVA powinien się koncentrować na substancjach niebezpiecznych wymienionych w:
    - Dyrektywie Seveso II i innych regulacjach dotyczących poważnych awarii.
    - Regulacjach dotyczących bezpieczeństwa zawodowego.
    - Statystykach działań terrorystycznych.
- Zbiorniki substancji chemicznych i wyposażenie, ich lokalizacja, objętość, średnia zawartość i konstrukcja.
- Założenia projektowe instalacji.
- Plany, wykresy; schematy rurowania, schematy systemów kontrolno pomiarowych , oraz schematy przepływów procesowych.
- Systemy zarządzania bezpieczeństwem, programy zarządzania ryzykiem.
- Analizy ryzyka na potrzeby ocen bezpieczeństwa.
- Informacje wspierające oszacowanie krytyczności zasobów w odniesiony do działów zakładu, instalacji; gospodarki regionu i kraju oraz możliwych skutków.
- Informacje o lokalizacji zakładu, obszarach zamieszkałych i środowiska w pobliżu zakładu, które mogą być narażone w razie zaistnienia zdarzenia z użyciem substancji chemicznych.
- Raporty dotyczące poprzednich wydarzeń z zakresu bezpieczeństwa. procesowego i działań niepożądanych.

Analiza skutków

Celem analizy skutków jest zrozumienie i oszacowanie potencjalnych strat, które mogą zaistnieć w przypadku udanego ataku terrorystycznego. Chemikalia, które zostały uwolnione do atmosfery, mogą przebyć duży dystans. Potencjalne skutki dotkną wówczas sąsiednie regiony, gdzie trzeba będzie ocenić szkody i zniszczenia. W przypadku ataku cybernetycznego, może zostać stracona część produkcji a procesy mogą zostać zatrzymane. Analiza skutków powinna zawierać rozległe informacje na temat możliwych scenariuszy uwolnienia. Dla każdego scenariusza uwolnienia, analiza powinna zawierać: oszacowanie potencjalnej ilości uwolnionej substancji oraz oszacowanie potencjalnych skutków z tym związanych dla pracowników, ludzi zamieszkałych lub przebywających w pobliżu oraz dla środowiska i dóbr materialnych. Punktem wyjścia dla takich ocen jest wyznaczenie zależności od odległości stężeń uwolnionej substancji lub wielkość promieniowania cieplnego i nadciśnienia, w przypadku towarzyszących uwolnieniu pożarów i wybuchów.

Ułatwieniem całego procesu analizy możliwych skutków może być przyjęcie zasady, że istnieją różne **typy zdarzeń** i odpowiednio dla nich **potencjalne cele:**

- Straty, szkody, skutki dla ludzi: potencjalnymi celami są: wyposażenie i sprzęty wykorzystywane w procesach bazujących na ropie naftowej i substancjach niebezpiecznych, tankowce, rurociągi i inne systemy transportowe, pracownicy, kontrahent, goście, zwłaszcza w większych skupiskach.
- Kradzież: potencjalne cele to: związki chemiczne w trakcie ich przetwarzania, magazynowania czy transportowania, wyposażenie stacji nadzorujących, czy systemy kontroli i inwentaryzacji, strategiczne informacje biznesowe w trakcie przekazywania ich droga telekomunikacyjną lub internetową.

- Zanieczyszczenia: potencjalne cele to: surowce, produkty końcowe i pośrednie procesów, emitowane zarówno przy ataku na magazyny, etapy procesu przetwórczego czy rurociągi strategiczne dane biznesowe i procesowe.
- Degradacja aktywów: potencjalne cele to: procesy wykorzystujące ropę naftową i inne substancje niebezpieczne, wizerunek zakładu oraz renoma jej marki, narzędzia i surowce, systemy telekomunikacyjne i systemy biznesowe.

Atrakcyjność celu

Atrakcyjność celu dla przeciwnika jest wskazówką dla zakładu, jak oceniać prawdopodobieństwo ataku. Dla przykładu może obejmować: bliskość symbolicznych celów, takich jak pomniki narodowe itp. i inne zmienne, kiedy zespół SVA zgadza się, że dane zajście ma wpływ na okoliczną ludność, zakład itp., wtedy musi przeprowadzić również analizę środków zaradczych i możliwych przeciwdziałań.

Pierścienie zabezpieczeń

Zespół SVA określa i dokumentuje istniejący poziom bezpieczeństwa w aspekcie możliwych działań terrorystycznych i stosowane pierścienie bezpieczeństwa w celach ochronnych (przykład stref obrazuje rys.1). Może to oznaczać bezpieczeństwo fizyczne, cybernetyczne, kontrole administracyjną i inne działania. Podczas tego kroku wszystkie działania, informacje i strategie realizowane są zbierane w specjalnej bazie informacyjnej.

Krok 3: Ocena zagrożeń terrorystycznych (threat assessment)

Istnieje wiele czynników determinujących oszacowywanie podatności danego obiektu na zagrożenia zewnętrzne. Zagrożenie może wynikać z łatwego dostępu do poszczególnych segmentów danego obiektu, z dostępności sąsiedztwa poszczególnych obiektów oraz ze względu na znaczenie strategiczne danego obiektu dla działalności całego zakładu. Do ataku może dojść zarówno w trakcie cyklu przetwórczego (procesy chemiczne, procesy produkcyjne, procesy wykorzystujące materiały niebezpieczne, systemy magazynowania) jak i podczas transportu (rurociągi, transport samochodowy, wodny i powietrzny). Ataki terrorystyczne mogą mieć charakter ogólny jak i specyficzny i indywidualny.

Zidentyfikowanie zagrożeń i możliwych ataków

Należy zidentyfikować aktywa i cele w obiekcie szczególnie narażone na akty terroru i sabotażu. Punktu widzenia SVA, identyfikacja zagrożeń związanych aktami terroru i sabotażu oznacza opracowanie modelu/scenariuszy takich działań z uwzględnieniem charakterystyk grup potencjalnych sprawców i ich zdolności realizacji zamierzeń.. Oszacowywanie podatności obiektu na potencjalne zagrożenia odbywa się z uwzględnieniem dostępnych środków bezpieczeństwa oraz dostępnych środków zaradczych.

Istnieje wiele czynników determinujących oszacowywanie podatności danego obiektu na zagrożenia zewnętrzne. Zagrożenie może wynikać z łatwego dostępu do poszczególnych segmentów danego obiektu, z dostępności sąsiedztwa poszczególnych obiektów oraz ze względu na znaczenie strategiczne danego obiektu dla działalności całego zakładu.

Do ataku może dojść zarówno w trakcie cyklu przetwórczego (procesy chemiczne, procesy produkcyjne, procesy wykorzystujące materiały niebezpieczne, systemy magazynowania) jak i podczas transportu (rurociągi, transport samochodowy, wodny i powietrzny). Ataki terrorystyczne mogą mieć charakter ogólny jak również specyficzny i indywidualny.

Grupy osób, które mogą być rozważane jako potencjalni sprawcy ataków terrorystycznych:
terroryści (lokalni i globalni); przestępcy; radykalni aktywiści; niebezpieczni indywidualiści; niezadowoleni pracownicy.

Terrorysta jest jednym z najbardziej trudnych przeciwników, gdyż może być dobrze wyszkolony, dobrze uzbrojony oraz przygotowany na śmierć, jeżeli umożliwiłoby to wykonanie zamierzonego celu Dla celów SVA, zagrożenie atakiem terrorystycznym powinno być rozważone jako najpierw, przed innymi zagrożeniami.

Jeżeli inne zagrożenie np. kradzież materiałów jest dużo bardziej prawdopodobne od ataku terrorystycznego, należy wtedy należy w pierwszym rzędzie przeprowadzić analizę motywacji działań i możliwości działań kryminalistów, a zagrożenia należy modelować w ten sam sposób jak zagrożenia terrorystyczne.

Tabela 1 przedstawia macierz możliwych zagrożeń (może być pomocna przy definiowaniu potencjalnego zagrożenia). W tabeli przedstawiono dziesięć zmiennych, począwszy od zamiaru przeciwnika, typu broni, jaką dysponuje, aż do zamierzonego celu. Pełna analiza SVA powinna uwzględniać wszystkie te scenariusze, które odnoszą się do poszczególnych obiektów krytycznych zakładu.

Charakterystyka zagrożeń

Ataki mogą przeprowadzać osoby wtajemniczone, osoby z zewnątrz bądź kombinacja tych obydwu typów. Do osób wtajemniczonych można zaliczyć personel, który zna procedury działania poszczególnych segmentów zakładów, a także mające dostęp do różnych części zakładu, do których dostępu bronią ściśle określone procedury. Zmowa między wymienionymi obydwoma typami osób atakujący może mieć miejsce gdy połączy je zysk finansowy, ideologia lub wystąpi przymus.

Charakterystyka przeciwnika jest pomocna w definiowaniu potencjalnych celów i posunięć osoby atakującej. Zespół przygotowujący analizy SVA powinien przeanalizować każdy z typów przeciwnika (zidentyfikowany wcześniej jako) pod względem jego wiarygodności, poziomu możliwości.

Tabela 1. Typy i znaczenie potencjalnych zagrożeń.

Nr zmiennej	**Zmienna**	**Opcje**
1	Rodzaj ataku	atak skierowany bezpośrednio na zakład; główny atak skierowany na inne obiekty poza zakładem, ze skutkami pośrednimi dla rozważanego zakładu.
2	Zakres zamierzonego celu lub cel pośredni	instalacje stacjonarne (procesy chemiczne, systemy produkcyjne, użytkownicy materiałów niebezpiecznych, systemy magazynowania); systemy łączności; systemy danych i informacji; zasoby finansowe; narodowe i strategiczne aktywa.
3	Przedmiot zamierzonego celu	życie ludzkie; obiekty publiczne; pracownicy zakładu; kadra kierownicza; przerwanie ciągłości pracy zakładu przechowywanie, użyłkowanie, lub przesyłanie informacji strategicznych; konta rozliczeniowe oraz zakładowe konta; wizerunek i reputacja zakładu; własność intelektualna, marka.
4	Strefy skutków	osoby prywatne; członkowie społeczności; cały zakład; personel zakładu; własność publiczna; własność zakładu; ciągłość działalności biznesowej; wpływy ekonomiczne; środowisko; wizerunek i opinia; własność intelektualna, marka.

5	Źródła zagrożeń	Zewnętrzny bezpośredni atak fizyczny – rozpoczęty na zewnętrz barier kontroli z zamiarem spowodowania bezpośredniej szkody (rakieta; materiał wybuchowy; zastosowanie broni z terenów przyległych zakładowi; staranowanie pojazdem głównej bramy; eksplozja rurociągu). Zewnętrzny pośredni atak fizyczny - rozpoczęty na zewnętrz barier kontroli z zamiarem spowodowania ogólnej szkody w zakładzie lub bezpośredniej szkody dla innych (zniszczenie obiektów sąsiadujących z zakładem ale będących łatwiejszym celem). Zewnętrzny pośredni atak wpływający na daną zakład - atak na główną infrastrukturę miejską wpływającą na funkcjonowanie zakładu (zniszczenie strategicznych elektrowni w mieście; zablokowanie sieci internetowych; zablokowanie systemu bankowego; przerwanie transportu, itp.). Wewnętrzny atak fizyczny– rozpoczęty od fizycznego naruszenia barier kontroli i umieszczenia ładunku wybuchowego w sąsiedztwie obiektu zakładu. Wewnętrzny atak fizyczny zainicjowany ze źródła umieszczonego wewnątrz obszaru chronionego przez bariery kontroli (np. sabotaż przez osoby, która pozostały na noc w budynkach zakładu).
6	Motyw	rząd przeprowadzający akcje militarne przeciwko terrorystom; założenia organizacji terrorystycznych; motyw osobisty powiązany z zakładem (niezadowolony pracownik); motyw osobisty nie powiązany z zakładem. (indywidualny sympatyk/fanatyk) • zbrodniczy zamiar (podpalenie; kradzież; morderstwo)
7	Typ broni	elektroniczne (zagrożenia internetowe – działania hakerów); działania fizyczne (otwarcie zaworu; uszkodzenie kabli komunikacyjnych); prywatny i publiczny transport – uszkodzenie ciężarówek, kolei, transportu lotniczego; wyposażenie zakładu – pojazdy spółki; otwarcie zaworu zbiorników magazynujących; przeprowadzenie reakcji emitującej znaczną ilość zanieczyszczeń; zatrucie produktu końcowego; broń ręczna - pistolet; broń automatyczna; strzelby; noże; broń dużego zasięgu –materiały wybuchowe; rakiety, granaty; broń dużego kalibru; broń masowego rażenia (broń jądrowa, biologiczna i chemiczna).
8	Wywołane skutki	elektroniczne; wybuchy i eksplozje; jądrowe; biologiczne; fizyczne;
9	Mechanizm wpływu	wpływ fizyczny; uwolnienie toksyczności/ kancerogenności uwolnionej substancji; pożar; eksplozja; wpływ elektroniczny. • Wpływ na łączność
10	Zamierzone Skutki	negatywny wpływ na społeczeństwo; negatywny wpływ na personel; osoby ranne wśród społeczeństwa; ranni wśród personelu; zakłócenie działania instytucji publicznych; zakłócenie normalnego działania zakładu; zanieczyszczenie środowiska straty finansowe; utrata danych; strata dobrej reputacji, znaczenia marki zakładu.

Krok 4: Analiza Podatności (vulnerability) – metoda wyboru celu lub scenariusza ataku

W trakcie tego kroku definiowane są podstawowe zagrożenia danego zakładu z uwzględnieniem prawdopodobieństwa ataku, a także ich „atrakcyjność" dla terrorysty. Jeżeli w trakcie analiz SVA jakieś zdarzenie zostanie określone jako dość prawdopodobne, należy dla niego określić także potencjalne jego scenariusze. Są dwie szkoły metodologii analiz: analizy oparte na scenariuszach i

analizy oparte na aktywach „atrakcyjnych” dla terrorysty. Zarówno w podejściu do analiz opartym na scenariuszu jak i na aktywach ostatecznym zadaniem jest uszeregowanie potencjalnych celów pod względem ryzyka ich zaatakowania, tzn. jak bardzo prawdopodobny jest atak uwzględniając wartość strategiczną celu, ale także dostępne środki zaradcze. Wszystkie scenariusze opracowane w Kroku 4 grupuje się w zestawy a następnie szereguje (obiekt, którego uszkodzenie ma największe skutki dla zakładu i środowiska przyrodniczego znajduje się na czele listy). Zespół powinien opracować takie zestawy, w których aktywa są współzależne z zagrożeniami.

Macierz aktywów/zagrożeń

Aktywa z listy krytycznych celów rozpatruje się pod kątem oceny zagrożenia, a odpowiednie zagrożenia i aktywa łączy się w pary tworząc macierz powiązań, lub wykorzystuje inne formy prezentacji powiązań między zagrożeniami, a aktywami zakładu. Krok ten ma na celu opracowanie podstawowego projektowego zagrożenia dla każdej instalacji zakładu.

Istnieją dwa podejścia: podejście oparte na scenariuszach i oparte na aktywach. Oba są prawie identyczne dla Kroków 1-3, ale różnią się stopniem szczegółowości analizy scenariuszy zagrożeń oraz specyficznymi przeciwdziałaniami stosowanymi w danym scenariuszu w Krokach 4-5. W obu podejściach identyfikuje się aktywa i analizuje skutki oraz atrakcyjność celów, jak w Kroku 2. Oba podejścia pozwalają uzyskać zbiór potencjalnych celów i oba podejścia mogą być równie skuteczne w ocenie podatności bezpieczeństwa i określeniu wymaganych zabezpieczeń.

Podejście oparte na aktywach

Podejście to jest podejściem „odgórnym”. W jego przypadku, szczegóły licznych scenariuszy mogących prowadzić do wystąpienia danych zdarzeń nie są rozpatrywane. Metoda ta zakłada także, że określanie i dokumentacja licznych scenariuszy jest działaniem opierającym się w znacznym stopniu na spekulacji ze względu na zmienny charakter dowolnego ataku i może to prowadzić do analizy środków zaradczych, która w zbyt dużym stopniu zajmuje się przewidywalnymi scenariuszami, nie rozpatrując przez to mniej oczywistych sposobów ataku.

Podejście to można stosować dla całej firmy o kilku zakładach, w szczególności, gdy charakteryzują się one podobnymi profilami zagrożeń i podatności. Na przykład podczas analizy skutków w Kroku 3 można było określić, że do wywołania z zadanej odległości zdarzenia o poważnych skutkach dla zbiornika z substancją niebezpieczną zdarzenia potrzeba by ok. 110 kg materiałów wybuchowych. Takie ilości materiałów wybuchowych zazwyczaj trzeba transportować przy pomocy pojazdu. W podejściu opartym na aktywach w tym miejscu kończy się wizualizacja zdarzenia, ponieważ dokładny przebieg zdarzeń prowadzących do umieszczenia ładunku wybuchowego takiej wielkości przy zbiorniku jest uważany za nieistotny. Minimalne środki bezpieczeństwa, w postaci betonowych barier i punktów kontroli dostępu mogą być rozmieszczone wokół zbiornika. Mogą one byś skutecznymi środkami zapobiegawczymi, a sam zbiornik będzie pod niższym ryzykiem uderzenia przez pojazd. W podejściu opartym na scenariuszu, które zostanie opisane poniżej, można wziąć ogólny scenariusz ataku na zbiornik przy pomocy pojazdu przenoszącego ładunek wybuchowy i rozszerzyć go tak, aby obejmował różne sposoby doprowadzenia do tego zdarzenia. Obie metody mogą doprowadzić do takich samych ogólnych wniosków dotyczących poziomu ryzyka, a także wybrać równoważne metody zapobiegawcze.

Ocena celów

Z opracowanej listy celów wybiera się do analizy najpierw cel o największych możliwych skutkach. Należy przy tym wziąć pod uwagę toksyczność, palność i wybuchowość chemikaliów. Pojedynczy cel może posiadać jedną, lub więcej z tych cech. W szczególności należy odpowiedzieć na pytanie, czy rozpatrywany materiał jest niebezpieczny:

- po uwolnieniu do atmosfery w odpowiedniej ilości może spowodować zgon znacznej liczby osób?

- po kradzieży jego dużej ilości może zostać wykorzystane do zaopatrzenia zakładu produkcji broni chemicznych o zasięgu regionalnym,
- po kradzieży jego małej ilości może zostać wykorzystane do produkcji prostych broni chemicznych bez wyrafinowanego sprzętu procesowego, których miejsce produkcji nie mogłoby zostać zidentyfikowane na podstawie użytych technologii,
- będąc przetwarzany, lub składowany jest podatny na sabotaż mogący prowadzić do niekontrolowanej reakcji, lub zagrożenia dla zdrowia i bezpieczeństwa ludzkiego.

czy też są to aktywa, które w razie niemożliwości wykorzystania spowodują zaprzestanie działania zakładu? Przykładami są:

- kluczowy sprzęt procesowy nie do zastąpienia;
- linie kredytowe;
- systemy komputerowe;
- inne zdarzenia katastroficzne.

Pytaniem, na które należy tutaj odpowiedzieć jest „Jakie rodzaje zdarzeń związanych z danym celem, np. rozerwanie zbiornika, zakłócenie procesu, utrata mocy, utrata chłodzenia, spowodują uwolnienie materiałów niebezpiecznych, w sposób powodujący wystąpienie najbardziej poważnych skutków?”. W razie potrzeby należy się wykorzystać istniejące analizy bezpieczeństwa, lub zagrożeń.

Należy pamiętać, że celowo wywołane zdarzenie mogące prowadzić do jednorazowego uwolnienia dużej ilości substancji może wykraczać poza zakres obecnych analiz uwolnień awaryjnych, przeprowadzanych na potrzeby raportów o bezpieczeństwie i planowania awaryjnego. Scenariusze uwolnienia określone dla uwolnień awaryjnych mogą nie być tak ciężkie jak scenariusze celowych uwolnień. Na przykład, dla scenariuszy uwolnień awaryjnych, rozsądne jest rozpatrywanie pojedynczego zbiornika, który traci swoją zawartość. W przypadku uwolnień wywołanych celowo, intensywność zdarzenia inicjującego, jak wybuch w pobliżu zbiorników, może spowodować uwolnienie zawartości wielu zbiorników i skutkować jeszcze dalszym położeniem tych samych punktów końcowych.

Rozpatruje potem możliwe warstwy ochronne dla potencjalnego celu, łącznie z zabezpieczeniami, oświetleniem, zachowaniem odległości od obszarów swobodnego dostępu, barierami, samą konstrukcją zbiornika i innymi czynnikami mającymi wpływ na potencjał ataku na dany zbiornik i jego potencjalne skutki. W miejscach, gdzie warstwy ochronne nie wystarczą do uniemożliwienia osobie atakującej wywołania poważnych skutków, potencjalny cel należy uznać za wysoce „opłacalny” dla osoby atakującej. Zadaniem jest identyfikacja Celów o Wysokiej Wartości i Wysoce Opłacalnych. Są to cele najbardziej podatne na atak. Cele, które mają Wysoką Wartość, lub są Wysoce Opłacalne (ale nie posiadają obu tych cech) można uznać za cele średnio podatne, a cele nie posiadające żadnej z tych cech za cele mało podatne.

Podejście oparte na scenariuszach

Podejście to korzysta z bardziej szczegółowej strategii analiz i wymaga dyskusji nad listą scenariuszy dla zrozumienia możliwych sposobów doprowadzenia do niepożądanego zdarzenia.

Początek podejścia opartego na scenariuszach jest identyczny jak w przypadku podejścia opartego na aktywach, ale różni się w stopniu szczegółowej analizy scenariuszy zagrożeń i specyficznych przeciwdziałań stosowanych do danego scenariusza. Dla obu podejść identyfikuje się aktywa, a atrakcyjność celów i skutki są analizowane jak w Kroku 2. Podejście oparte na scenariuszach rozpatruje pytanie: „w jaki sposób cel może być zaatakowany” przez opracowanie specyficznych scenariuszy ataków.

Podejście oparte na scenariuszach obejmuje określenie rodzajów osób/organizacji, które mogłyby przeprowadzić atak na dany cel oraz ocenę prawdopodobieństwa, że aktualny system zabezpieczeń zniechęci, wykryje i opóźni atak zanim zostanie udanie przeprowadzony

W tym miejscu konieczne jest przeprowadzenie konserwatywnej oceny aktualnych możliwości systemu zabezpieczeń. Przykładowo:

- czy aktualny zakładowy system kontroli dostępu będzie w stanie *wykryć* oszustów posługujących się fałszywymi dokumentami, lub strojem?
- czy aktualny system kontroli dostępu będzie w stanie *wykryć* broń, lub materiały wybuchowe?
- czy aktualne środki ochronne będą w stanie *opóźnić* lub *zneutralizować* działania atakującego w świetle jego cech i zdolności?

Ocenia się prawdopodobieństwo powodzenia ataku. Skala oceny jest względna i prosta: wysokie, średnie, lub niskie prawdopodobieństwo.

Prawdopodobieństwo Powodzenia Ataku jest w tym przypadku w całości oparte na zdolności aktualnego systemu zabezpieczeń do uniemożliwienia danego ataku. Opracowanie scenariuszy, powinno być realizowane przy pomocy systematycznej metody i przejrzyście udokumentowane. Scenariusze można dokumentować różnorako. Jednym ze sposobów jest Podejście „Co-gdy"/List Kontrolnych, w którym scenariusze dla każdego celu umieszcza się w formularzu, a pytania powyżej sformułowane są dla sprowokowania dyskusji dotyczącej możliwych środków ataku celu.

Można tu skorzystać z systematycznego zbioru zagrożeń opartego na czterech głównych kategoriach zdarzeń:

- Uwolnienie niebezpiecznych chemikaliów w zakładzie wskutek zamierzonego uszkodzenia sprzętu, lub celowe uwolnienie chemikaliów mogące powodować wiele ofiar, poważne szkody i skutki dla środowiska lub społeczeństwa.
- Kradzież substancji chemicznej, lub nieprawidłowe zastosowanie w celu wyrządzenia poważnych szkód w zakładzie, lub poza nim.
- Zanieczyszczenie lub zepsucie w inny sposób produktów w celu wyrządzenia szkód dla pracowników, lub społeczeństwa wewnątrz zakładu, lub poza nim.
- Uszkodzenie aktywów, lub infrastruktury, lub zmniejszenie funkcji lub wartości biznesowej zakładu, lub całego zakładu przez działania terrorystyczne.

Zbiornik można zaatakować na różne sposoby prowadzące do każdego z wyżej wymienionych punktów. Ogólne scenariusze dla każdego z nich są omawiane, a później Zespół APZ analizuje istniejące dla każdego scenariusza zabezpieczenia mające na celu zapobiegnięcie, wykrycie i zniechęcenie atakujących. Każdy scenariusz ocenia się pod kątem prawdopodobieństwa i spodziewanej wagi zdarzenia. Zespół APZ przegląda wszystkie postulowane scenariusze i określa, które są reprezentatywne. Te scenariusze są wówczas w pełni analizowane, rozwijane i dokumentowane przez Zespół APZ do celów oceny podatności.

Ranking/ Ocena Ryzyka

W obu powyższych podejściach do Oceny Podatności końcowym krokiem jest określenie poziomu ryzyka udanego ataku na dany obiekt przy uwzględnieniu istniejących zabezpieczeń. Scenariusze opracowane podczas Kroku 4 grupuje się w *Zbiory Zabezpieczeń* wg celów. Listy scenariuszy powinny być zorganizowane wg wagi ich skutków. Należy udokumentować scenariusze ataku opracowane dla każdego zbioru zabezpieczeń, na przykład:

Przykład Zbiorów Zabezpieczeń

Zbiór zabezpieczeń	1
Obiekt	Zbiornik
Zagrożenie	Bezpośredni atak pojazdem z urządzeniem wybuchowym
Skutki	Katastroficzne

Poziom ryzyka scenariuszy jest ustalany w oparciu o prostą skalę 1-3 lub 1-5. Można skorzystać także z macierzy ryzyka, która ustala rangę każdego scenariusza w oparciu o jego prawdopodobieństwo i skutki. Celem jest kategoryzacja aktywów w dyskretnych poziomach ryzyka tak, aby dla każdej sytuacji można było zastosować odpowiednie przeciwdziałania.

Krok 5: Analiza środków zaradczych

Podejście oparte na aktywach przedstawiało scenariusze ogólne z odgórnym założeniem określonych dostępnych środków zaradczych. W podejściu opartym na scenariuszu środki zaradcze są określane dla każdego scenariusza osobno. Niezależnie jednak od stosowanego podejścia należy określić ilość i właściwości dostępnych środków zaradczych, aby móc stworzyć hierarchię zagrożeń. Przeprowadzenie analizy środków zaradczych jest potrzebne, aby określić różnicę pomiędzy istniejącymi a pożądanymi środkami bezpieczeństwa oraz zdefiniował gdzie istnieje potrzeba zwiększenia tychże środków.

3. PODSUMOWANIE

Bezpieczeństwo instalacji stacjonarnych, odnoszące się do niepożądanych interwencji stron trzecich powinno opierać się na szczegółowo opracowanym planie bezpieczeństwa, zawierającym wytyczne pozwalające zminimalizować m.in. zagrożenia terrorystyczne i sabotażowe oraz pomagające w efektywnym przydzielaniu środków poprzez: identyfikowanie aktualnych i potencjalnych źródeł zdarzeń, zagrożeń aktami terroru i sabotażu, mogących powodować zagrożenie dla prawidłowej pracy instalacji; identyfikowanie prawdopodobieństwa i skutków potencjalnych zdarzeń z udziałem instalacji stacjonarnych; prowadzenie wyczerpującej i zintegrowanej oceny, testującej i porównującej całe spektrum potencjalnych zdarzeń oraz nakreślającej możliwe sposoby zapobiegania i redukowania skutków awarii; prowadzenie konstruktywnej, łatwo dostępnej oceny bezpieczeństwa w celu ułatwienia dostępu, wyboru i implementacji najlepszych metod redukujących ryzyko; ustalenie i śledzenie rozwoju planu bezpieczeństwa zwłaszcza pod względem wdrażania głównych założonych celów; ustanowienie standaryzowanych warunków bezpieczeństwa i dokonywania kontrolnych pomiarów osiągów dla zmniejszenia ryzyka wystąpienia zagrożenia. Zespół opracowujący plan bezpieczeństwa powinien kierować się następującymi zasadami: plan bezpieczeństwa dla instalacji stacjonarnych powinien być elastyczny; integracja informacji jest naczelną zasadą pozwalającą stworzyć sprawnie funkcjonujący plan bezpieczeństwa Analizy SVA stanowią podstawę do opracowania planów bezpieczeństwa obejmujących działania prewencyjne i zalecenia sposobu reagowania w przypadku wystąpienia ataku.

Dodatki do materiału: „Algorytm szacowania podatności na uszkodzenie instalacji procesowej wskutek aktów terroru i sabotażu oraz propozycje metod oceny zagrożeń" zawierają listy kontrolne i rodzaje formularzy wraz ze wskazaniem sposobu przyporządkowania punktów w ramach analiz odpowiadających wyżej wymienionych kroków 2-5. Na ich podstawie można tworzyć indeksy podatności, atrakcyjności obiektów, prawdopodobieństwa ataku terrorystycznego i skutków. Na tej podstawie można opracować zestawienia w postaci analogicznej do macierzy ryzyka.

Literatura

[1] Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, August 2002

[2] M. Borysiewicz, A. Wasiuk**,** Algorytm szacowania podatności na uszkodzenie instalacji procesowej wskutek aktów terroru i sabotażu oraz propozycje metod oceny zagrożeń. Materiały niepublikowane, CIOP PIB, 2005.