Marek Barć
Rzeszów University of Technology

RODZAJE OCHRONY INFRASTRUKTURY KRYTYCZNEJ

STRESZCZENIE

Ochrona infrastruktury krytycznej to proces, który obejmuje dużą liczbę obszarów zadaniowych i kompetencji oraz angażujący wiele zainteresowanych stron. Proces ten obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej, zakłada również stopniowe dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie[1].

Słowa kluczowe:
infrastruktura krytyczna, ochrona, system ochrony, plan ochrony

WSTĘP

Ochrona IK obejmuje zapobieganie zagrożeniom i ograniczanie ich skutków, zmniejszanie podatności infrastruktury krytycznej na zagrożenia oraz szybkie przywrócenie jej prawidłowego funkcjonowania na wypadek wszelkich zdarzeń mogących je zakłócić[2]. Niniejszy artykuł w sposób syntetyczny określa rodzaje ochrony infrastruktury krytycznej, współpracę w realizacji zadań i dobre praktyki ochrony IK.

OCHRONA FIZYCZNA

Ochronę fizyczną powinna wykonywać wewnętrzna służba ochrony lub podmioty działające zgodnie z ustawą z dnia 22 sierpnia 1997 r. o ochronie

[1] Cz. Znamierowski, *Rozważania o państwie,* Warszawa 1999, s. 60.
[2] Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007r (Dz. U. z 2007 nr 89 poz. 590 z późn. zm.).

osób i mienia[3]. Zapewni to m.in. możliwość użycia, środków przymusu bezpośredniego przez osoby wykonujące tę ochronę. Wykonywanie tych zadań realizuje się przez zapewnienie ciągłej, 24-godzinnej ochrony fizycznej obiektów, urządzeń, instalacji i systemów IK. Jednym ze sposobów na ochronę fizyczną IK jest podział terenu, na strefy ochrony (strefy ograniczonego dostępu) i zaplanowanie ich zgodnie z zasadą ochrony w głąb. Każda ze stref musi być zaprojektowana w celu spowolnienia działań potencjalnego napastnika, a natężenie sił i środków ochrony musi rosnąć w miarę zbliżania się potencjalnych napastników do strefy chroniącej kluczowe elementy infrastruktury organizacji. W rezultacie może to zniechęcić napastnika lub da więcej czasu na odpowiedź systemu ochrony lub wykwalifikowaną pomoc. Podział stref ochrony można zaplanować następująco:

1) specjalna strefa bezpieczeństwa;
2) strefa bezpieczeństwa;
3) strefa chroniona;
4) strefa kontrolowana.

Niezależnie od stref ochrony lub w przypadku braku wydzielenia takich stref, niezbędne będzie określenie warunków, w których następuje wzmocnienie poziomu ochrony przez zastosowanie dodatkowych środków ochrony, w tym przede wszystkim organizacyjnych i proceduralnych.

W celu wzmocnienia ochrony należy również wprowadzić procedury dotyczące:

1) zasad wejścia do stref ochrony pracowników oraz pojazdów obsługujących oraz sposób poruszania się po obiekcie, obejmujące: dostęp do poszczególnych stref ochrony przez autoryzację przez system kontroli dostępu lub zgodnie z innymi zastosowanymi elementami rejestracji i identyfikacji np. pobieranie kluczy za potwierdzeniem lub zastosowania kodu PIN lub możliwość przeszukania;
2) zasad użycia elementów identyfikacji (klucze/kody/PIN/karty), obejmujące: rejestrację elementów identyfikacji, zasady przechowywania oraz wydawania kluczy do pomieszczeń i stref chronionych, okresową wymianę kodów, tryb wydawania i przyznawania kart;
3) wydawania przepustek oraz nadawania uprawnień oraz ich zdejmowania użytkownikowi;
4) zasad wejścia kontrahentów i wjazdu pojazdów do nich należących, obejmujące: nadanie uprawnień na wejście i rejestrację kontrahentów, możliwość przeszukania, zasad poruszania się po obiekcie;
5) zasad wejścia gości i wjazdu pojazdów do nich należących, obejmujące: nadanie uprawnień na wejście i rejestrację odwiedzających, zasady poruszania się po obiekcie, wizualną identyfikację;

[3] Ustawa o ochronie osób i mienia z 22 sierpnia 1997r (Dz. U. z 2005 nr 145, poz. 1221 z późn. zm.)

6) kontroli środków ochrony, obejmujące: odpowiedzialnych za kontrole, odstępy czasu między kontrolami, protokoły pokontrolne itp.;
7) serwisowania technicznych środków ochrony fizycznej, obejmujące: okresową obsługę zgodnie z dokumentacją techniczną, określone umownie czasy usuwania usterek itp.

Modele ochrony fizycznej[4]

Ochronę fizyczną można organizować w system posterunków (doraźnych lub stałych) oraz patroli. W trakcie ochrony osoby pełniące służbę wykonują: patrole piesze wewnątrz i na zewnątrz obiektu, patrole samochodowe, kontrole ruchu osobowego, kontrole przesyłek oraz ruchu samochodowego.

Wyróżnia się trzy podstawowe modele ochrony fizycznej, które można podzielić pod względem rozmieszczenia i poziomu mobilności jednostek ochrony:

1) model statyczny;
2) model ruchomy;
3) model mieszany.

Celem modelu statycznego jest uniemożliwienie osobom postronnym zajęcia terenu przez określony okres czasu i jest on preferowany w sytuacji, gdy utrata obiektu jest niedopuszczalna. Cechuje się wielowarstwową ochroną, wielowarstwowym systemem wykrywania oraz stałymi posterunkami ochronnymi.

Charakterystyką modelu ruchomego[5] jest to, że służby ochrony swobodnie poruszają się po obiekcie i reagują na pojawiające się alarmy lub podejrzane zachowanie, używane są różne systemy elektroniczne uzupełniające działania służb ochrony oraz mogą swobodnie poruszać po całym obiekcie.

Z kolei model mieszany zawiera cechy obu modeli opisanych powyżej i sprawdza się szczególnie w przypadku dużych obiektów. Cechuje go wielowarstwowa ochrona, zgranie elementów ochrony statycznej z ruchomymi patrolami oraz stałymi posterunkami ochronnymi w strefie „zero".

Pracownicy realizujący ochronę fizyczną IK, powinni dokumentować zdarzenia i sytuacje mogące zagrażać bezpieczeństwu chronionego mienia.

Jeśli istnieje taka możliwość, obiekty infrastruktury krytycznej powinny być całkowicie ogrodzone. Ogrodzone powinny być również wyznaczone strefy ochrony. Ogrodzenie powinno spełniać wymogi jak najdłuższego czasu pokonywania przez potencjalnego napastnika więc w tym celu należy doprowadzić do sytuacji aby:

[4] Załącznik nr 2 do Narodowego Planu ochrony Infrastruktury Krytycznej, s. 19.
[5] www.rcb.gov.pl [dostęp: 05.02.2021]

1) wysokość ogrodzenia nad powierzchnią terenu powinna w maksymalny sposób utrudnić jego pokonanie ponad nim;
2) dolną krawędź ogrodzenia należy zabetonować lub w inny sposób trwale zamontować w podłożu bądź osadzić w podmurówce;
3) ogrodzenie powinno być wyposażone w próg uniemożliwiający dokonanie podkopu;
4) powinno być wyposażone w bariery wieńczące ogrodzenie z drutu kolczastego lub spirali drutu ostrzowego[6].

Dostęp do stref ochrony oraz kluczowych pomieszczeń lub obszarów powinien być kontrolowany i ograniczony wyłącznie do uprawnionych osób. Zdolność do takich działań zapewniają systemy kontroli dostępu, które[7]:

1) umożliwiają zabezpieczanie przed nieuprawnionym dostępem do stref ochrony;
2) umożliwiają poruszania się po obiekcie osób, które są do tego upoważnione;
3) umożliwiają wydzielenia stref ochrony, do których dostęp będą miały tylko osoby upoważnione;
4) umożliwiają monitoring czasu przebywania w strefie,
5) wspomagają potwierdzanie tożsamości pracowników;
6) zapewniają odpowiedni poziom praw dostępu dla kontrahentów i gości[8].

Telewizja przemysłowa CCTV to system kamer służących do przekazywania obrazu z określonych stref, obszarów lub pomieszczeń w zamkniętym systemie odbiorczym, służący do nadzoru oraz zwiększeniu bezpieczeństwa stref, obszarów lub pomieszczeń. Telewizja przemysłowa sprawdza się w przypadku, kiedy wybrane strefy, obszary lub pomieszczenia wymagają stałej kontroli i nadzoru. Zastosowanie telewizji przemysłowej pozwala na:

1) prowadzenie działań ochronnych z oddalonych miejsc;
2) identyfikację rodzaju zdarzenia;
3) wykrycie i identyfikację osób oraz pojazdów;
4) detekcję ruchu;
5) zapis materiałów audio i wideo.

Systemy sygnalizacji włamania i napadu (SSWiN) stosuje się w celu wykrycia i rejestracji prób nielegalnego wejścia do stref ochrony, wybranych obszarów i pomieszczeń. SSWiN oparte są na urządzeniach:

1) wykrywających ruch w strefie objętej ich działaniem;
2) sygnalizujących otwarcie drzwi;

[6] B. Kędzia, *Zabezpieczenia w dobie terroryzmu,* "Zabezpieczenia" nr 3/2007.
[7] http://wiadomości. gazeta.pl/wiadomości/1,114873,13212796, Super szpieg_w_sieci czy _Red October_ szperal _w_systemach.html [dostęp: 10.03.2021]
[8] http://alewandal.pl/infrastruktura-krytyczna [dostęp: 10.03.2021].

3) sygnalizujących wypełnienie otworów budowlanych (wejścia, okna, inne otwory);
4) sygnalizujących uszkodzenie powierzchni szklanych;
5) ostrzegających o zagrożeniach (przyciski alarmowe).

OCHRONA TECHNICZNA

Ochrona techniczna infrastruktury krytycznej to zespół przedsięwzięć, które mają na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej. Oznacza to, że ochrona techniczna IK obejmuje m.in.:

1) sprawy związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi przepisami i normami np. budowlanymi i przeciwpożarowymi,
2) działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług,
3) działania techniczne mające na celu zapewnienia ciągłości funkcjonowania IK.

Właściciel lub zarządca obiektu budowlanego w tym przypadku jest obowiązany:

1) utrzymywać i użytkować obiekt zgodnie z zasadami, o których mowa powyżej;
2) zapewnić, dochowując należytej staranności, bezpieczne użytkowanie obiektu w razie wystąpienia czynników zewnętrznych oddziaływujących na obiekt, związanych z działaniem człowieka lub sił natury.

Dla obiektów, w których zlokalizowane są elementy infrastruktury krytycznej należy przyjmować najwyższe wymagania dotyczące niezawodności zasilania i dostępu do mediów[9].

OCHRONA OSOBOWA

Ochrona osobowa to zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z osobami, które przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu.

Podstawą skuteczności ochrony osobowej jest zebranie jak największej liczby informacji, możliwych do uzyskania w świetle obowiązującego prawa,

[9] R Sośnicki, *Cyberterroryzm a infrastruktura krytyczna państwa*, AON 2011, s. 7.

o potencjalnym pracowniku już w procesie rekrutacji. Warto przeprowadzić ocenę ryzyka zakłócenia funkcjonowania IK, związanego z nielegalnym wykorzystaniem informacji lub praw dostępu dla różnych stanowisk w strukturze organizacji.

Na tożsamość osoby składają się przymioty nadawane po narodzeniu (imię, nazwisko, data i miejsce urodzenia, imiona rodziców), indywidualne cechy biometryczne (biometria linii papilarnych, tęczówki, dłoni, twarzy, DNA) oraz elementy biografii (historia edukacji, zatrudnienia). Obowiązkowo należy wymagać dokumentów trudnych do podrobienia, takich jak: paszport, dowód osobisty czy prawo jazdy.

Sprawdzenie kwalifikacji kandydata powinno opierać się o weryfikację informacji zawartych w dokumentach rekrutacyjnych (CV, formularze itp.). Pozwoli to ocenić wiarygodność i uczciwość kandydata oraz zdobyć informacje, które chciałby ukryć. Należy porównać, czy zgadzają się informacje opisane w CV z przedstawianymi świadectwami, certyfikatami itp. Uwagę winno się zwrócić na nazwę szkoły, uczelni, firmy. Podobną procedurę należy przeprowadzić przy sprawdzaniu doświadczenia zawodowego. Wymagać należy podania historii zatrudnienia z okresu co najmniej 3 lat[10]. Wykorzystując narzędzie badawcze, jakim są testy psychologiczne (w odniesieniu do stanowisk, co do których realizacja testów jest zasadna) i narzędzia psychometryczne, można ocenić osobowość kandydata, możliwości analityczne – predyspozycje do określonej pracy.

W przypadku rekrutacji na kluczowe stanowiska, połączone z dostępem do informacji niejawnych, postępowanie sprawdzające przeprowadzają właściwe służby ochrony państwa. Nie należy jednak zaniedbywać wewnętrznego procesu weryfikacji kandydata.

Priorytetem w ochronie osobowej jest dokładne sprawdzenie pracownika jeszcze przed jego zatrudnieniem, nie wolno zaniedbywać jednak zasad bezpieczeństwa w stosunku do już zatrudnionych w organizacji. Jednym z podstawowych sposobów na ochronę osobową IK jest ograniczanie dostępu pracowników organizacji do wrażliwych miejsc lub zasobów znajdujących się na terenie organizacji, jak i w sieciach teleinformatycznych. Osoby odpowiedzialne za bezpieczeństwo w ustalonych odstępach czasu powinny:

1) weryfikować prawa dostępu i w razie potrzeby je ograniczać,
2) kontrolować, analizować i raportować wszelkie próby nieautoryzowanego dostępu do miejsc (pomieszczeń) oraz sieci i zasobów teleinformatycznych.

[10] W. Wojciechowicz, *Ochrona infrastruktury krytycznej państwa*, "Myśl Wojskowa",1/2004, s. 17.

Pracownicy organizacji powinni być uczuleni na próby nieautoryzowanego dostępu wszelkich osób do zastrzeżonych miejsc oraz informować odpowiedzialne osoby o zauważonych tego typu próbach.

Identyfikacja wizualna pracowników organizacji oraz podwykonawców i gości jest najprostszym sposobem określenia przynależności do organizacji oraz potencjalnych uprawnień. Każda osoba znajdująca się w obiekcie należącym do IK powinna nosić w widocznym miejscu identyfikator zawierający fotografię twarzy posiadacza.

W każdej organizacji są osoby posiadające newralgiczną (unikalną) wiedzę na temat jej funkcjonowania oraz doświadczenie i „pamięć instytucjonalną". Są one szczególnie cenne dla organizacji, a jednocześnie stanowią potencjalnie największe zagrożenie na wypadek działania na niekorzyść organizacji.

Pracownicy podmiotów, wykonujący pracę na zlecenie operatora IK, powinni zostać zweryfikowani w podobny sposób, jak w przypadku rekrutacji, a dodatkowo należy sprawdzić, czy dany podwykonawca jest członkiem rozpoznawalnego i uznanego stowarzyszenia, posiada odpowiednie licencje, spełnia standardy jakości, posiada stabilność finansową itp.

Każdy z pracowników odchodzących z organizacji jest w posiadaniu mniej lub bardziej wrażliwej wiedzy, która może być wykorzystana w nielegalny sposób. Opuszczający stanowisko pracownik powinien zwrócić:

1) odzież firmową, w tym umundurowanie;
2) identyfikatory, przepustki;
3) służbowe telefony komórkowe;
4) służbowe karty kredytowe;
5) służbowe wizytówki;
6) klucze do pomieszczeń;
7) generatory kodów jednorazowych;
8) należące do organizacji dokumenty;
9) przenośne dyski danych, komputery.

OCHRONA TELEINFORMATYCZNA

Ochrona teleinformatyczna infrastruktury krytycznej to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych. Cyberataki na systemy IK stały się częścią konfliktów cybernetycznych w cyberprzestrzeni, w tym konfliktów między państwami[11].

[11] Zob. W. Leśnikowski, *Cyberatak na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania rozwiniętych państw,* www.cdis.wp.mil.pl/pl25_133 html [dostęp: 12.03.2021]

Istnieje wiele modeli identyfikacji cech, jakie powinien spełniać prawidłowo chroniony system teleinformatyczny. Jednym z bardziej znanych i najczęściej używanych jest system wskazujący na trzy najważniejsze cechy bezpieczeństwa:

1) poufność;
2) integralność;
3) dostępność.

Szczególnymi zagrożeniami dla tak rozumianego modelu bezpieczeństwa są:

1) nieuprawniony dostęp do informacji i procesów jako naruszenie ich **poufności;**
2) zmiana lub inne zakłócenie informacji i wykonywanych procesów jako naruszenie ich **integralności;**
3) blokada dostępu do informacji i procesów jako naruszenie ich **dostępności.**

Najistotniejszymi elementami ochrony teleinformatycznej IK są[12]:

1) Współpraca sektorowa;
2) Plany awaryjne i ciągłości działania;
3) Bezpieczeństwo oprogramowania;
4) Kontrola dostępu;
5) Ochrona stacji roboczych;
6) Bezpieczeństwo sieci bezprzewodowych;
7) Monitoring zagrożeń;
8) Reakcja na incydenty.

1. Współpraca sektorowa

Znaczna część IK znajduje się w rękach sektora prywatnego. Często organizacje władające IK są na rynku komercyjnym konkurentami. Niemniej jednak zasada konkurencji nie powinna dotyczyć kwestii bezpieczeństwa.

2. Plany awaryjne i ciągłość działania

Plany awaryjne zapewniające ciągłość działania powinny być przygotowywane i utrzymane wg przedstawionego schematu. W tej fazie najważniejszym zadaniem jest ustalenie tych zasobów, które powinny być uwzględnione w planach awaryjnych. Jest to zadanie ściśle związane z oceną ryzyka. W fazie opracowania rozwiązania powstają szczegółowe plany, które odpowiadają na pytania: kiedy? kto? co? w jaki sposób? Opracowując te plany, trzeba pamiętać, że nie wszystkie sytuacje da się przewidzieć w fazie planowania. Po tym, jak zostaną opracowane plany awaryjne, powinna nastąpić ich implementacja.

[12] W. Cieślak, *Analiza zagrożeń czynami przestępczymi oraz szacowania ryzyka*, dwumiesięcznik "Ochrona mienia i informacji", nr 4/2005.

Właściwym rozwiązaniem jest, aby wraz z implementacją nastąpiło przetestowanie zaplanowanych rozwiązań. Właściwa weryfikacja planów odbywa się w fazie testów. W tym przypadku w testowaniu uczestniczą wszyscy zainteresowani. Testy te mogą być mniej lub bardziej złożone. Test prosty może składać się z uruchomienia pojedynczej procedury awaryjnej obejmującej nie więcej niż 3 komórki organizacyjne[13]. Przykładowy scenariusz może uwzględniać:

- awarię głównego serwera pocztowego organizacji,
- atak wirusa unieruchamiającego komunikaty alarmowe przekazywane z systemu SCADA,
- awarię systemu kontroli fizycznej wejścia do budynku.

3. Bezpieczeństwo oprogramowania

Zasady zapewnienia bezpieczeństwa oprogramowania opierają się na uniwersalnych zasadach, które dotyczą również zapewnienia bezpieczeństwa dla innych zasobów teleinformatycznych, a przede wszystkim systemu operacyjnego. Najważniejszymi elementami zapewnienia bezpieczeństwa oprogramowania są:

- testowanie oprogramowania w wydzielonym środowisku, przed wdrożeniem produkcyjnym,
- aktualizacja systemu operacyjnego,
- aktualizacja oprogramowania,
- testowanie zmian wynikających z aktualizacji,
- audyt bezpieczeństwa kodu,
- współpraca z dostawcą oprogramowania.

4. Kontrola dostępu

Kontrola dostępu do zasobów jest podstawowym sposobem ochrony systemu teleinformatycznego. Główną zasadą, jaką należy się kierować przy ustalaniu zasad dostępu do zasobów, jest zasada „potrzeby dostępu do informacji" (ang. *need to know).* W szczególności chodzi o zastosowanie wirtualnych sieci lokalnych (ang. *Virtual Local Network),* czyli sieci komputerowych wydzielonych logicznie w ramach większej sieci fizycznej. Dzięki takiemu wydzieleniu możliwa jest separacja ruchu sieciowego, co jest ważną zasadą ochrony. Firewalling jest jedną z podstawowych technik bezpieczeństwa. Realizowany jest on w oparciu o odpowiednie oprogramowanie lub kompletne rozwiązanie w postaci dedykowanego urządzenia i oprogramowania. Zarówno przy pomocy wirtualnych sieci lokalnych, jak i firewallingu, możemy stworzyć rozwiązanie polegające na separacji sieci bezpośrednio obsługującej IK organizacji. Jako sieć

[13] M. Brożyna, *Polityka Bezpieczeństwa Informacji w przedsiębiorstwach o szczególnym znaczeniu gospodarczo-obronnym*, dwumiesięcznik, Ochrona mienia i informacji, nr 4/2005.

bezpośrednio obsługującą IK rozumiemy tę część sieci organizacji, w której przetwarzane są kluczowe dane i obsługiwane są obiekty, urządzenia, instalacje stanowiące właściwą IK. Dostęp do zasobów organizacji z zewnątrz powinien odbywać się w sposób bezpieczny, pamiętając głównie o dostępie szyfrowanym (wybór protokołów i algorytmów szyfrujących powinien być dokonany na podstawie ich podatności na ataki kryptoanalityczne) i opartym o mocne uwierzytelnienie. Jedną z możliwych do wyboru metod kontroli dostępu jest tworzenie „czarnych list" i „białych list". Wykorzystanie tych technik jest często w ochronie antyspamowej. Również można je stosować w przypadku ochrony przed złośliwym oprogramowaniem instalującym się bez wiedzy użytkownika w trakcie odwiedzin zainfekowanej strony www.

Kolejną techniką kontroli dostępu jest użycie serwera pośredniczącego. Oprócz funkcji bezpieczeństwa może on również spełniać zadania poprawy efektywności ruchu, np. przez pośredniczenie w dostępie do zasobów internetowych, które jeśli były wcześniej ściągane przez jednego użytkownika, to dla kolejnych są już udostępniane z serwera pośredniczącego, a nie z oryginalnego serwisu, co znacznie przyśpiesza transmisję danych[14].

W sieciach obsługujących IK nadal bardzo popularnym sposobem dostępu do urządzeń jest dostęp dodzwaniany (ang. *dial-up).* W przypadku korzystania z dostępu dodzwanianego należy zwrócić uwagę na zapewnienie następujących zasad bezpieczeństwa:

- kontrolę danych logowania,
- kontrolę dostępu z wykorzystaniem odpowiednio mocnego hasła, w miarę możliwości hasła jednorazowego,
- systemu wykrywania połączeń z nieautoryzowanych źródeł i alarmowania o nich.

5. Ochrona stacji roboczych

Powszechność dostępu do sieci Internet przez stacje robocze pracowników organizacji powoduje znaczny wzrost podatności na zagrożenia z niej pochodzące. Dlatego rekomendowanym rozwiązaniem jest rezygnacja z możliwości dostępu ze stacji roboczych pracowników, podłączonych do Internetu, do systemów obsługujących IK.

Najlepiej, jeśli będzie się odbywała w sposób automatyczny. Należy zwrócić uwagę, że oprócz powszechnej świadomości związanej z koniecznością aktualizacji oprogramowania systemów operacyjnych, konieczne jest również aktualizowanie aplikacji. Uzupełnieniem dla aktualizacji oprogramowania

[14] Dane z wystąpienia przedstawiciela Rządowego Centrum Bezpieczeństwa podczas konferencji "*Bezpieczeństwo energetyczne państwa a infrastruktura krytyczna na przykładzie PGNiG i GAS-SYSTEM*, która odbyła się w Wojskowej Akademii Technicznej 23 maja 2012 r.

i ochrony typu *firewalling* jest ochrona przed złośliwym oprogramowaniem. Wśród złośliwego oprogramowania można wyróżnić:

- wirusy komputerowe (ang. *computer virus),*
- robaki internetowe (ang. *Internet worms),*
- konie trojańskie (ang. *trojan horse),*
- oprogramowanie szpiegujące (ang. *spyware),*
- oprogramowanie kradnące tożsamość (ang. *crimeware).*

6. Bezpieczeństwo sieci bezprzewodowych

Sieci bezprzewodowe ze względu na łatwość budowy i konfiguracji oraz wygodę użycia są bardzo rozpowszechnione. Wykorzystanie sieci bezprzewodowych, bez zastosowania odpowiednich zabezpieczeń, niesie ze sobą duże zagrożenia, w szczególności możliwość:

- nielegalnego wykorzystania tych sieci do działań przestępczych,
- nieuprawnionego dostępu do informacji innych podmiotów.

Warto również zwrócić uwagę, że bezpieczeństwo sieci bezprzewodowych powinno być rozpatrywane nie tylko z punktu widzenia własnych sieci, ale również sieci obcych, wykorzystywanych przez pracowników naszej organizacji. Wyłączenie komunikacji z sieci bezprzewodowych do sieci obsługujących IK lub zasobów stanowiących IK jest skutecznym sposobem zmniejszenia ryzyka zakłócenia funkcjonowania IK. W sieciach bezprzewodowych powinno być stosowane szyfrowanie komunikacji. Najpopularniejszymi standardami szyfrowania są standardy WEP (*Wired Equivalent Privacy) and WPA/WPA2 (Wi-Fi Protected Access).* Standardy WPA2 są standardami bezpieczniejszymi i one są rekomendowane[15]. Podstawą cyberataku na sieć bezprzewodową jest wykrycie tej sieci, dlatego wyłączenie rozgłaszania tzw. SSID sieci (*service set identifier),* choć nie zapewni pełnego bezpieczeństwa, z pewnością utrudni skuteczny cyberatak. Zezwolenie na dołączenie do sieci bezprzewodowej tylko tych urządzeń, których adres fizyczny MAC został wcześniej wpisany jako adres dozwolony.

Poprawa bezpieczeństwa sieci bezprzewodowych w organizacji możliwa jest również przez fizyczne ograniczenie dostępu do sieci tzn. takie kształtowanie sygnału radiowego, aby był on dostępny tylko i wyłącznie z wybranych lokalizacji. Oprócz zapewnienia bezpiecznego korzystania z własnej sieci bezprzewodowej ważne jest, aby korzystanie z sieci innych podmiotów również odbywało się w sposób bezpieczny.

[15] K. Kowalczyk, *Cenna ochrona,* "Polska Zbrojna" z 16 stycznia 2011r.

7. Monitoring zagrożeń

Niezależnie od tego, jak silnie będzie zabezpieczona nasza sieć teleinformatyczna, możliwość przeprowadzenia skutecznego cyberataku na nią zawsze istnieje. Dlatego organizacja powinna prowadzić stały monitoring zagrożeń.

Następujące rodzaje urządzeń można wykorzystać do organizacji systemu monitoringu zagrożeń i wczesnej reakcji na ich wystąpienie:

- Systemy detekcji zagrożeń sieciowych IDS (ang. *Intrusion Detection System)*
- Możliwe jest zastosowanie dwóch rodzajów systemów typu IDS:
- HIDS (ang. *Host Based Intrusion Detection System)* – system wykrywania zagrożeń sieciowych przeznaczony dla wybranych urządzeń (np. kluczowych serwerów),
- NIDS (ang. *Network Intrusion Detection System)* – system wykrywania zagrożeń sieciowych przeznaczony dla wybranych sieci (może być np. zlokalizowany na styku sieci lokalnej z Internetem).

Monitoring zagrożeń powinien zostać zorganizowany dla ochrony kluczowych zasobów firmy. Standardowe rozmieszczenie odpowiednich systemów monitorujących powinno obejmować następujące logiczne lokalizacje w sieci organizacji:

- styk z siecią Internet,
- styk z siecią, w której odbywa się zarządzanie (w ramach wewnętrznej organizacji),
- najważniejsze urządzenia obsługujące IK.

8. Reakcja na incydenty

Istotną kwestią organizacyjną jest powołanie w strukturach organizacji zespołu do spraw reagowania na przypadki naruszania bezpieczeństwa teleinformatycznego zwanego CERT (ang. *Computer Emergency Response Team)* lub *CSIRT (Computer Security Incident Response Team).*

Po odpowiednim okresie funkcjonowania zespołu (np. po 6 miesiącach) powinna nastąpić ocena tej funkcjonalności. Ocena ta pozwoli odpowiedzieć na to, czy warto było powoływać do życia taką komórkę i jeżeli odpowiedź jest twierdząca, to co ewentualnie warto poprawić w jej funkcjonowaniu[16].

Procedura obsługi incydentów może być bardziej lub mniej skomplikowana. Dobrym rozwiązaniem jest rozpoczęcie działania ze stosunkowo prostą procedurą, która będzie rozwijana i udoskonalana wraz z rozwojem zespołu.

[16] Ibidem, s. 110.

WNIOSKI

Jednym z głównych zadań bezpieczeństwa wewnętrznego jest zagwarantowanie funkcjonalności systemom infrastruktury krytycznej. Ochrona infrastruktury krytycznej, tak istotna dla bezpieczeństwa państwa i jego obywateli, jest również najważniejszym zadaniem stawianym przed szefami administracji rządowej jak i samorządowej. Dostęp do tego rodzaju usług staje się sprawą kluczową z punktu widzenia sprawnego funkcjonowania i rozwoju nowoczesnego państwa, społeczeństwa i gospodarki. Usługi te oraz dostarczająca je infrastruktura zostały określone mianem infrastruktury krytycznej.

W wyniku zdarzeń spowodowanych siłami natury lub działaniami człowieka infrastruktura krytyczna może ulec zniszczeniu lub uszkodzeniu. Konsekwencją może być zagrożenie ciągłości świadczenia kluczowych usług, a tym samym mienia, zdrowia lub nawet życia obywateli. Biorąc pod uwagę również fakt, że incydenty tego typu negatywnie wpływają na rozwój gospodarczy państwa, należy stwierdzić, że infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, a jej ochrona jest jednym z priorytetów stojących przed państwem polskim.

Niezależnie od rozwiązań przyjętych przez państwo, należy podejmować wszelkie działania prawne minimalizujące ryzyko zakłócenia funkcjonowania IK. Zapewnienie sobie tytułu prawnego do nieruchomości na której zlokalizowana jest IK, pozwalające na egzekwowanie dostępu do IK oraz zabezpieczenia się umowami z dostawcami mediów, są przykładami dobrych praktyk w tym zakresie.

BIBLIOGRAFIA

[1] Brożyna M., Polityka Bezpieczeństwa Informacji w przedsiębiorstwach o szczególnym znaczeniu gospodarczo-obronnym, dwumiesięcznik, Ochrona mienia i informacji, nr 4/2005.
[2] Cieślak W., Analiza zagrożeń czynami przestępczymi oraz szacowania ryzyka, dwumiesięcznik "Ochrona mienia i informacji", nr 4/2005.
[3] Kędzia B., Zabezpieczenia w dobie terroryzmu, "Zabezpieczenia" nr 3/2007.
[4] Kowalczyk K., Cenna ochrona, "Polska Zbrojna" z 16 stycznia 2011.
[5] Leśnikowski W., Cyberatak na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania rozwiniętych państw, www.cdis.wp.mil.pl/pl25_133 html.
[6] Piwowarczyk R., Ochrona infrastruktury krytycznej, www.uwm.edu.pl
[7] Pyznar M., Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury - wizja Rządowego Centrum

Bezpieczeństwa, [w:] Ochrona infrastruktury krytycznej, red. A. Tyburska, Wyższa Szkoła Policji, Szczytno 2010.
[8] Sośnicki R., Cyberterroryzm a infrastruktura krytyczna państwa, AON 2011.
[9] W. Wojciechowicz., Ochrona infrastruktury krytycznej państwa, "Myśl Wojskowa",1/2004.
[10] Znamierowski Cz., Rozważania o państwie, Warszawa 1999.
[11] Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007r (Dz. U. z 2007 nr 89 poz. 590 z późn. zm.).
[12] Ustawa o ochronie osób i mienia z 22 sierpnia 1997r (Dz. U. z 2005 r. nr 145, poz. 1221 z późn. zm.).
[13] Załącznik nr 2 do Narodowego Planu ochrony Infrastruktury Krytycznej, www.rcb.gov.pl
[14] http://wiadomości. gazeta.pl/wiadomości/1,114873,13212796, Superszpieg_w_sieci czy _Red October_ szperal _w_systemach.html
[15] http://alewandal.pl/infrastruktura-krytyczna.
[16] http://rcb.gov.pl/?page_id=210.
[17] Dane z wystąpienia przedstawiciela Rządowego Centrum Bezpieczeństwa podczas konferencji "*Bezpieczeństwo energetyczne państwa a infrastruktura krytyczna na przykładzie PGNiG i GAS-SYSTEM*, która odbyła się w Wojskowej Akademii Technicznej 23 maja 2012 r.

TYPES OF CRITICAL INFRASTRUCTURE PROTECTION

ABSTRACT

One of the main tasks of internal security is to guarantee the functionality of the critical infrastructure systems. The protection of critical infrastructure, so important for the security of the state and its citizens, is also the most important task for the heads of government and local government administration. Access to this type of services becomes a key issue from the point of view of the efficient functioning and development of a modern state, society and economy. These services and the infrastructure that provides them have been referred to as critical infrastructure.

As a result of events caused by natural or human activities, critical infrastructure may be destroyed or damaged. The consequence may be a threat to the continuity of key services, and thus the property, health or even life of citizens. Taking into account also the fact that such incidents negatively affect the economic

development of the state, it should be stated that the critical infrastructure plays a key role in the functioning of the state and the life of its citizens, and its protection is one of the priorities for the Polish state.

Critical infrastructure protection is a process that covers a large number of task areas and competences, and involves many stakeholders. This process includes all activities aimed at ensuring functionality and continuity of activities and integrity of the critical infrastructure, it also assumes a gradual achievement of the expected result and continuous improvement.