ZESZYTY NAUKOWE WSOWL

Nr 2 (148) 2008 ISSN 1731-8157

Artur SZLESZYŃSKI*

ORGANIZACYJNY ASPEKT BEZPIECZEŃSTWA INFORMACJI W INFORMATYCZNYCH SYSTEMACH WSPOMAGAJĄCYCH PROCES DOWODZENIA – ZARZĄDZANIA

Wstęp

W obszarze technicznych środków dowodzenia ważne miejsce zajmują informatyczne środki wspomagające proces dowodzenia na szczeblu ZT. Zadaniem systemów wspomagających proces dowodzenia jest gromadzenie, obróbka oraz prezentacja wyników przetwarzania danych przez system teleinformatyczny. Miarą bezpieczeństwa informacji jest zapewnienie przez obsługę systemu odpowiedniego poziomu atrybutów bezpieczeństwa informacji, jakimi są: poufność, integralność, dostępność[1].

System bezpieczeństwa informacji składa się z dwóch aspektów: organizacyjnego i technicznego. Aspekt organizacyjny identyfikuje zagrożenia dla bezpieczeństwa informacji oraz definiuje zasady postępowania z ryzykiem. Dokumentacja systemu bezpieczeństwa informacji opisuje procedury eksploatacji oraz działania naprawcze w systemie, określając np. oczekiwany (akceptowany) czas przestoju dla podsystemów krytycznych.

Aspekt techniczny odpowiada za techniczne wykonanie zaleceń zawartych w dokumentacji bezpieczeństwa wybranego systemu. Rolą aspektu technicznego jest wypełnianie funkcji dotyczących inżynierii zabezpieczeń w systemie[2].

Realizacja aspektu organizacyjnego wymaga połączenia wysiłku różnych komórek organizacyjnych instytucji. W przypadku stanowiska dowodzenia jednostki podmiotami partycypującymi w pracy nad dokumentacją systemu będą żołnierze znajdujący się w sztabie jednostki, przedstawiciele batalionu (plutonu) dowodzenia oraz pionu Pełnomocnika do spraw ochrony informacji niejawnych[3]. W literaturze dotyczącej bezpieczeństwa informacji fakt angażowania w proces opracowania dokumentacji systemu

* kpt. mgr inż. Artur SZLESZYŃSKI – Wyższa Szkoła Oficerska Wojsk Lądowych

1 ISO/IEC15408, s. vii.

2 R. Anderson, *Inżynieria zabezpieczeń*, Warszawa 2005, s. 4.

3 A. Białas, *Bezpieczeństwo informacji i usług we współczesnej firmie i instytucji*, Warszawa 2007, s. 87.

bezpieczeństwa tak znacznej liczby osób tłumaczy się odpowiedzialnością wszystkich użytkowników za ochronę funkcjonowania systemu[4]. Drugim celem jest kształtowanie świadomości użytkowników systemu związanej z jego niezawodną eksploatacją oraz ograniczenie postawy określanej zdaniem „bezpieczeństwo informacji to nie my, to zadanie Pełnomocnika ds. ochrony informacji niejawnych". Dobrze opracowana dokumentacja systemu bezpieczeństwa może zostać wykorzystana w procesie szkolenia użytkowników z zakresu problematyki bezpieczeństwa informacji oraz zostanie użyta do przygotowania audytu bezpieczeństwa informacji[5].

Kwestie związane z dokumentacją systemu bezpieczeństwa reguluje Ustawa o ochronie informacji niejawnych, która dla systemów teleinformatycznych przetwarzających informacje niejawne nakazuje opracowanie dokumentów, jakimi są Szczegółowe Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji. Opracowanie wymienionych dokumentów należy oprzeć na analizie ryzyka oraz ocenie wpływu zagrożeń na funkcjonowanie polowego zautomatyzowanego systemu dowodzenia (PZSyD).

Ochrona informacji w zautomatyzowanym polowym systemie dowodzenia

Systemy wspomagające procesy dowodzenia należą do grupy zasobów krytycznych w obszarze technicznych środków dowodzenia. Gromadzone, przetwarzane i przechowywane w nich informacje mają kluczowe znaczenie dla efektywności procesu dowodzenia. Ponieważ opisane rozwiązanie zawiera dane dotyczące zasobów osobowych oraz elementów wsparcia logistycznego oddziału, na podstawie Ustawy o ochronie informacji niejawnych, klasyfikowany jest jako zasób przetwarzający dane o klauzuli - co najmniej - zastrzeżone[6]. Jedną z funkcjonalności, w systemach wspomagania dowodzenia, jest konieczność współpracy z zewnętrznymi systemami informatycznymi np. systemami rodzajów wojsk, systemami wsparcia dowodzenia sił sojuszniczych.

Dokumentacja systemu bezpieczeństwa powinna regulować kwestie związane z zapewnieniem odpowiedniego poziomu atrybutów bezpieczeństwa informacji we wszystkich prawdopodobnych wariantach wykorzystania PZSyD. Proces tworzenia systemu bezpieczeństwa informacji rozpoczyna analizy ryzyka, która wskazuje zagrożenia dla bezpieczeństwa informacji przetwarzanej i przesyłanej w teleinformatycznym systemie wspomagania dowodzenia. Na podstawie analizy zagrożeń oraz ilościowych i jakościowych metod oceny ryzyka tworzona jest strategia postępowania z ryzykiem[7]. W przypadku zabezpieczania stanowisk dowodzenia należy rozważyć opracowanie standardowego szablonu zabezpieczeń, który będzie wdrożony we wszystkich stanowiskach dowodzenia. Uzasadnieniem dla wprowadzenia szablonu jest możliwość zdefiniowania jednolitych zasad konfiguracji stacji roboczych, serwerów oraz elementów infrastruktury teleinformatycznej, co ułatwi kontrolę rozwiązania.

Kolejnym zadaniem dokumentacji systemu bezpieczeństwa informacji jest przygotowanie wymagań do przeprowadzenia audytu bezpieczeństwa informacji w syste-

---

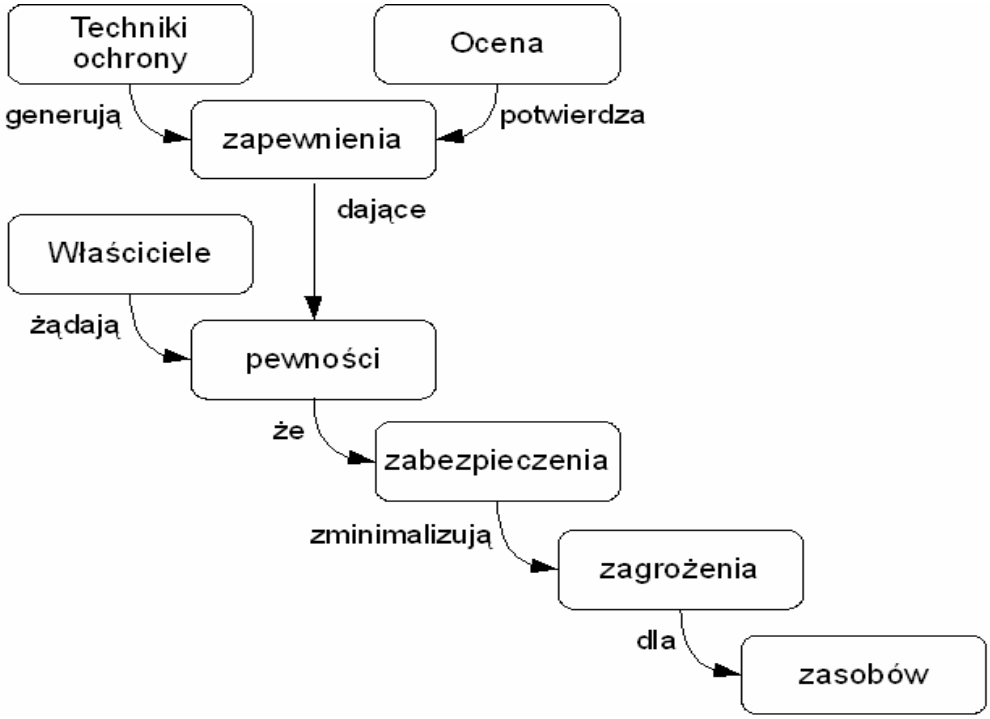
4 Tamże, s. 80.

5 K. Liderman, Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?, [w:] „Biuletyn IAR" nr 21/2004, s. 83.

6 Ustawa z dn. 22.01.1999 „O ochronie informacji niejawnych" art. 23.

7 A. Białas, op. cit., s. 90.

mie. Definiując zadania audytu bezpieczeństwa informacji, należy podać miary pozwalające jednoznacznie stwierdzić, czy informacja jest odpowiednio chroniona[8]. Miary będą potwierdzeniem (dla właściciela zasobu), że wdrożone środki ochrony właściwie wypełniają powierzone funkcje oraz że przewidywany wpływ zagrożenia na chroniony zasób jest minimalny, rys. 1.



Rys. 1. Koncepcja oceny bezpieczeństwa oraz relacji pomiędzy właścicielami, technikami ochrony a chronionymi zasobami

Źródło: Standard ISO/IEC-15408

Kwestia zdefiniowania miary poziomu bezpieczeństwa jest jednym z trudniejszych zadań, jakie powinny zostać wykonane przez zespół opracowujący szablon dokumentacji systemu bezpieczeństwa. Wynika to z faktu, iż informacja nie ma postaci materialnej i wykrycie kradzieży lub wycieku informacji jest trudne. Szablon wprowadzając standardowy sposób postępowania z ochroną informacji, wskazywałby zadania, jakie musi wypełnić administrator polowego zautomatyzowanego systemu dowodzenia, w zakresie kontroli występowania incydentów w bezpieczeństwie teleinformatycznym. Wiedzę o zdarzeniach negatywnych w systemie teleinformatycznym można czerpać z analizy incydentów w eksploatowanych systemach wsparcia dowodzenia oraz raportów technicznych firm zajmujących się kwestiami bezpieczeństwa[9].

Analiza ryzyka

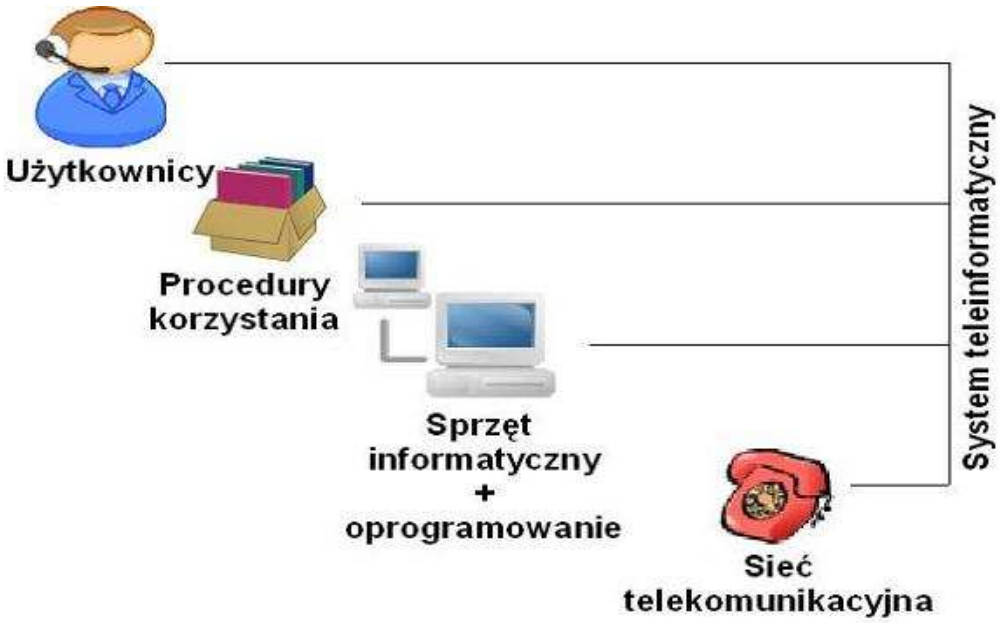
System teleinformatyczny wspomagający proces dowodzenia składa się z nastę-

[8] K. Liderman, op. cit., s. 82.

[9] Raport techniczny instytutu SANS dotyczący 20 najgroźniejszych podatności w systemach operacyjnych (www.sans.org). Symantec Internet Security Threat Report , [online]. [dostęp: 2008] Dostępny w internecie: http: /www.symatec.com./. I. Jóźwiak, W. Laskowski, Statistical Analysis of Security Attributes of Computer Systems, s. 570.

pujących elementów, rys. 2:

- użytkowników,
- procedur korzystania,
- sprzętu informatycznego (komputery, drukarki, urządzenia sieciowe itp.),
- oprogramowania,
- sieci telekomunikacyjnej.



Rys. 2. Elementy systemu teleinformatycznego

Źródło: Opracowanie własne

Każdy z wymienionych elementów charakteryzuje się występowaniem podatności, które mogą zostać wykorzystane przez zagrożenia, prowadząc do wystąpienia incydentu w bezpieczeństwie teleinformatycznym. Wykrycie podatności oraz jej usunięcie, jest jednym z najtrudniejszych zadań stawianych przed administratorami i użytkownikami polowego zautomatyzowanego systemu dowodzenia.

Obiektem (obiektami) podlegającym szczególnej ochronie są zasoby kluczowe (określane również terminem zasoby krytyczne), których zatrzymanie, zniszczenie lub utrata powodują wystąpienie znacznych szkód w systemie oraz we współpracujących z nimi rozwiązaniami.

W systemie wsparcia dowodzenia do zasobów krytycznych należy zaliczyć:

- użytkowników systemu,
- personel odpowiedzialny za administrację systemem,
- sprzęt komputerowy,
- infrastrukturę teleinformatyczną,
- infrastrukturę telekomunikacyjną,
- oprogramowanie wykorzystane w systemie (serwer bazy danych, serwer pracy grupowej, system operacyjny serwera i terminali użytkowników, oprogra-

mowanie komunikacyjne),

- informację przechowywaną, przetwarzaną i przesyłaną przez elementy systemu,
- wiedzę tworzoną na podstawie zgromadzonych informacji.

Ochrona wymienionych zasobów jest warunkiem koniecznym do poprawnego przebiegu procesu dowodzenia. Zniszczenie lub znaczny ubytek któregoś z wymienionych zasobów będzie skutkowało perturbacjami w pracy organu dowodzenia. Organ dowodzenia stawia przed systemem łączności następujące wymagania operacyjno - taktyczne:

- terminowość,
- wierność,
- skrytość[10].

Rolą technicznych środków dowodzenia jest transmisja zadań poza obszar stanowiska dowodzenia (zewnętrzne więzi informacyjne) oraz sprawna wymiana informacji na terenie stanowiska dowodzenia (wewnętrzne więzi informacyjne). Analizując wymienione wymagania, można stwierdzić, iż dotyczą one niezawodnego i bezpiecznego funkcjonowania systemu dowodzenia.

Należy zatem określić, jakich zagrożeń dla bezpieczeństwa informacji można oczekiwać i jakie potencjalne negatywne skutki takie zagrożenie może wyrządzić. Na potrzeby publikacji użyto jakościowej metody oceny ryzyka bazującej na technice drzewa użyteczności[11].

Analiza zagrożeń bezpieczeństwa informacji w polowych systemach wspomagania procesu dowodzenia, wykonywana jest w powiązaniu z atrybutami bezpieczeństwa informacji. Przykładowe zagrożenia dla bezpieczeństwa informacji przedstawiono w tabeli 1.

Tabela 1. Przykładowe zagrożenia dla bezpieczeństwa informacji

Atrybut bezpieczeństwa informacji	***Lp.***	***Opis zagrożenia***	***Istotność i szacowany skutek zagrożenia***
Poufność	1.	Dostęp osób nieupoważnionych do informacji np. w postaci papierowej	L, M
	2.	Nieprzestrzeganie zasad kryptograficznej ochrony przesyłanych informacji	M,H
	3.	Nieprzestrzeganie zasad ochrony przed emisjami ujawniającymi	L,M
	4.	Złamanie, przez przeciwnika, systemu ochrony kryptograficznej przesyłanych informacji	L,H

[10] J. Michniak, *Dowodzenie i łączność*, Warszawa 2005, s. 106.

[11] I. Jóźwiak, Wykorzystanie drzewa użyteczności..., [w:] „Zeszyty Naukowe Politechniki Śląskiej", Gliwice 2008.

Atrybut bezpieczeństwa informacji	*Lp.*	*Opis zagrożenia*	*Istotność i szacowany skutek zagrożenia*
	5.	Zagubienie lub zabór przenośnych urządzeń umożliwiających dostęp do systemu teleinformatycznego	M,M
	6.	Ujawnienie poufnych informacji świadome lub nieświadome	L,H
	7.	Dopuszczenie do eksploatacji systemu osób nieposiadających odpowiednich umiejętności w obsłudze oprogramowania	M,H
	8.	Nadanie zbyt wysokich uprawnień użytkownikowi w dostępie do zasobów serwera bazy danych i zasobów dyskowych	M,H
	9.	Obecność oprogramowania złośliwego w systemie informatycznym	L,H
	10.	Występowanie podatności w systemie operacyjnym i modułach polowego zautomatyzowanego systemu dowodzenia	M,H
	11.	Utrata kopii bezpieczeństwa danych przechowywanych w systemie wspomagania dowodzenia	L,H
Dostępność	1.	Brak kopii bezpieczeństwa danych składowanych na dyskach twardych w serwerze systemu w miejscu przywracania systemu	H,H
	2.	Przechowywanie ważnych danych na lokalnych dyskach twardych komputerów użytkowników	M,M
	3.	Brak funkcji replikacji danych pomiędzy węzłami sieci teleinformatycznej	M,H
	4.	Uszkodzenie serwera lub infrastruktury teleinformatycznej	M,H
	5.	Zniszczenie elementów składowanych systemu teleinformatycznego przez grupy dywersyjne lub ostrzał artylerii przeciwnika	H,H
	6.	Błędy w kopii bezpieczeństwa	L,H
	7.	Nieprzygotowany plan przywracania do działania systemu teleinformatycznego	H,H

Atrybut bezpieczeństwa informacji	*Lp.*	*Opis zagrożenia*	*Istotność i szacowany skutek zagrożenia*
	8.	Brak zapasowego sprzętu teleinformatycznego pozwalającego na przywrócenie systemu do działania	H,H
	9.	Stosowanie zakłóceń w celu obezwładnienia systemu radiokomunikacyjnego	M,M
	10.	Brak kompetentnej obsługi serwerowni oraz systemu telekomunikacyjnego	M,H
	11.	Nieprzestrzeganie procedur rejestracji incydentów w systemie teleinformatycznym, np. nieinformowanie administratora o niepoprawnej pracy oprogramowania	M,L
Integralność	1.	Działania celowe lub przypadkowe użytkowników systemu teleinformatycznego	M,H
	2.	Odebranie wiadomości zakłóconej lub błędna klasyfikacji wiadomości	M,M
	3.	Zmiana treści wiadomości wskutek występowania zakłóceń w kanale telekomunikacyjnym	L,L
	4.	Działania oprogramowania złośliwego (wirusy, key logger)	L,H
	5.	Niepoprawna klasyfikacji treści wiadomości przez system statystycznej weryfikacji treści wiadomości	L,L

Zagrożenia, które powinny podlegać w pierwszej kolejności eliminacji lub redukcji, są oznaczone literami {H,H}. Do tej grupy należą zagrożenia:

- zniszczenie elementów składowanych systemu teleinformatycznego przez grupy dywersyjne lub ostrzał artylerii przeciwnika,
- brak kopii bezpieczeństwa danych składowanych na dyskach twardych w serwerze systemu w miejscu przywracania systemu,
- nieprzygotowany plan przywracania do działania systemu teleinformatycznego.

Wysoka istotność informuje, że prawdopodobieństwo wystąpienia zagrożenia jest wysokie, zaś negatywny skutek dla systemu jest również wysoki. Zniszczenie elementów składowych np. zniszczenie serwerowni lub aparatowni zapewniającej dostęp do sieci telekomunikacyjnej będzie skutkowało przestojem w funkcjonowaniu stanowiska dowodzenia. Brak planu przywracania do działania systemu spowoduje, że próba szybkiego odtworzenia stanu sprzed zdarzenia będzie trudna lub niemożliwa. Jeżeli nie zostały przygotowane środki pozwalające na przywrócenie do działania (kopie bezpie-

czeństwa danych składowanych w serwerze stanowiska dowodzenia, zapasowy sprzęt, itp.), nie wskazano, które zasoby programowe i sprzętowe powinny zostać odtworzone oraz nie określono maksymalnego akceptowanego czasu przestoju, to jak można zweryfikować czy odtworzenie informatycznego systemu wsparcia dowodzenia jest możliwe.

Kolejne zagrożenia brane do eliminacji lub redukcji są opisane wartościami {H,M} lub {M,H}. Zagrożenia te mają wysokie lub średnie prawdopodobieństwo wystąpienia. Wysokie lub średnie są, dla systemu, konsekwencje wystąpienia zagrożenia. Najniżej w rankingu zagrożeń znajdują się zdarzenia oznaczone etykietą {L,L}, czyli posiadające niskie prawdopodobieństwo wystąpienia oraz niski poziom negatywnych skutków dla bezpieczeństwa informacji. Eliminacją lub ograniczeniem ich wpływu na system można zająć się po wyeliminowaniu lub zredukowaniu zdarzeń zaklasyfikowanych, jako wysoce prawdopodobne i posiadające duży poziom szacowanych szkód.

Miary bezpieczeństwa informacji

Pierwszą miarą bezpieczeństwa systemu jest czas przywrócenia do działania podsystemów zaklasyfikowanych do grupy zasobów kluczowych. Informacja ta powinna być umieszczona w Planie awaryjnego działania, który powinien stanowić niejawną część Szczegółowych Wymagań Bezpieczeństwa. Niejawność wynika z faktu, iż informacja ta adresowana jest tylko do administratora systemu.

Miarą bezpieczeństwa informacji jest liczba incydentów dotyczących błędów w dostępie (logowaniu się) użytkownika do zasobów serwera. Należy stwierdzić czy źródłem incydentu jest jeden i ten sam użytkownik, czy grupa użytkowników. Zadanie to będzie miało szczególne znaczenie w momencie segmentowania LSK[12] w celu umożliwienia pracy osobom spoza etatowej obsady stanowiska dowodzenia. Reakcją na cyklicznie pojawiający się incydent może być zablokowanie dostępu użytkownika do sieci teleinformatycznej. Przed zablokowaniem konta użytkownika należy sprawdzić poprawność konfiguracji stacji roboczej (roboczych) oraz jej podłączenie do urządzeń aktywnych sieci teleinformatycznej.

Zdarzeniem, które należy monitorować, jest próba uzyskania dostępu do informacji realizowana przy użyciu urządzeń końcowych podłączonych do węzła łączności stanowiska dowodzenia. Incydent ten jest atakiem socjotechnicznym polegającym na podszywaniu się przez intruza pod osobę posiadającą zwierzchność nad atakowanym. W procedurach bezpiecznej eksploatacji dla danego stanowiska należy dokładnie określić kto, kiedy i na jakich zasadach może uzyskać dostęp do określonych rodzajów informacji. Zasada ta wprowadza pewne utrudnienie w komunikacji wewnątrz stanowiska dowodzenia, jednak w przypadku korzystania z niechronionych kryptograficznie relacji łączności, ogranicza zagrożenie nieświadomego ujawnienia poufnych informacji.

Miarą bezpieczeństwa informacji jest liczba wykrytych incydentów związanych z obecnością oprogramowania złośliwego. Może się wydawać, że tego typu incydenty nie powinny pojawiać się w sieciach pracujących autonomicznie. Badania przeprowadzone na stacji roboczej pracującej autonomicznie (nieposiadającej podłączenia do sieci zewnętrznej np. Internet) wykazały pojawienie się incydentów związanych z obecnością wirusów[13]. Źródłem oprogramowania złośliwego są użytkownicy podłączający do kom-

[12] LSK – lokalna sieć komputerowa stanowiska dowodzenia.

[13] I. J. Jóźwiak, W. Laskowski, Statistical Analysis of Security Attributes of Computer Systems [w:]

putera prywatne urządzenia do przechowywania danych (dyski zewnętrzne, pendrive'y). Ponieważ sieci teleinformatyczne stanowisk dowodzenia będą podłączone do systemów stacjonarnych, ryzyka wystąpienia oprogramowania złośliwego nie można ignorować. Środkiem zaradczym jest stosowanie oprogramowania antywirusowego, które powinno neutralizować działanie złośliwego oprogramowania.

We wstępie do referatu stwierdzono, że jedną z funkcjonalności systemów wsparcia procesu dowodzenia jest ich interoperacyjność z systemami zewnętrznymi, należy liczyć się z koniecznością wystąpienia zagrożeń ze strony oprogramowania złośliwego przenoszonego w trakcie wymiany danych. Planując działania związane z ograniczeniem negatywnych skutków wystąpienia incydentów związanych z działaniem złośliwego oprogramowania, należy, oprócz wymienionego wcześniej oprogramowania antywirusowego, stosować odpowiednią konfigurację stacji klienckich. Ważnym elementem są szkolenia dla użytkowników podnoszące poziom świadomości i kształtujące pożądane zachowania.

Integralność przesyłanych informacji wpływa na szybkość klasyfikowania i przetwarzania informacji. Jednym z zagrożeń, z jakimi można się spotkać w PZSyD, jest celowe niszczenie integralności wiadomości przesyłanych za pomocą kanału radiowego. Atakujący liczy, że niwelując integralność meldunków i rozkazów, paraliżuje system dowodzenia. Zwiększająca się liczba incydentów, których źródłem jest brak integralności przesyłanych danych, może sugerować, że przeciwnik stara się rozpoznać system ochrony kryptograficznej przesyłanych wiadomości. Inną przyczyną zwiększonego występowania wymienionego typu zdarzeń może być związane z prowadzeniem ataku mającego na celu rozsychronizowanie rozmyto widmowego systemu radiokomunikacyjnego. Duża liczba wiadomości mylnie klasyfikowanych powinna wymusić zmianę procedur ochrony kryptograficznej przesyłanych wiadomości. Kolejnym działaniem powinna być rekonfiguracja systemu telekomunikacyjnego ujęta w planie awaryjnego działania. W kwestiach dotyczących poufności przekazywanych informacji administrator LSK powinien ściśle współpracować z komórkami odpowiedzialnymi za bezpieczeństwo i zarządzanie systemem łączności.

Zaproponowane miary bezpieczeństwa mają pomóc administratorowi LSK w ocenie poziomu bezpieczeństwa informacji w zarządzanej sieci. Miary stanowią wzorzec, który będzie wykorzystany w procedurach oceny bezpieczeństwa. Do wykonania powyższego zadania potrzebna będzie metodyka oceny poziomu bezpieczeństwa informacji w LSK. Zdaniem autora zadanie opracowania metodyki należy powierzyć komórce organizacyjnej w Dowództwie Wojsk Lądowych lub na szczeblu Ministerstwa Obrony Narodowej. Jednolite procedury oceny poziomu bezpieczeństwa LSK bazujące na jednolitych procedurach konfiguracji serwerów, stacji roboczych oraz urządzeń aktywnych sieci teleinformatycznej pozwoli na zapewnienie odpowiedniego jednolitego poziomu bezpieczeństwa teleinformatycznego w Wojskach Lądowych.

W celu osiągnięcia i utrzymania określonego poziomu sprawności teleinformatycznego systemu wspomagającego proces dowodzenia konieczne jest szkolenie administratorów i użytkowników. Warunek ten, choć oczywisty, często jest marginalizowany. Analiza liczby incydentów występujących w systemach teleinformatycznych poka-

---

"International Journal of Reliability, Quality and Safety Engineering, Special Issue on SSARS 2007" vol. 14, Number 6, December 2007, s. 571.

zuje, że 70%[14] zdarzeń spowodowana jest przez niewłaściwą obsługę systemu oraz zaniedbania organizacyjne dotyczące eksploatacji systemu teleinformatycznego.

Należy pamiętać, że środowisko, w którym eksploatowany jest polowy zautomatyzowany system dowodzenia, znacznie odbiega od środowiska, w którym eksploatowane są systemy teleinformatyczne stacjonarne. Konieczność zmian miejsca pracy wynikająca z dynamiki sytuacji bojowej nie sprzyja bezpieczeństwu teleinformatycznemu polowego zautomatyzowanego systemu dowodzenia. Występują zagrożenia, których nie uwzględnia się w systemach teleinformatycznych stacjonarnych, polegające na fizycznym eliminowaniu elementów systemu teleinformatycznego. Silny stres występujący u użytkowników oraz personelu odpowiedzialnego za nadzór i konfigurację systemu może być źródłem podatności, które mogą stać się przyczyną występowania incydentów w bezpieczeństwie informacji. Rozwiązaniem opisanego problemu może być taka konfiguracja systemu, która będzie ograniczała destrukcyjne działania użytkowników.

Podsumowanie

Aspekt organizacyjny bezpieczeństwa informacji pozwala na eliminację części incydentów występujących w systemach wspomagania dowodzenia. Na podstawie zapisów umieszczonych w Procedurach Bezpiecznej Eksploatacji użytkownik powinien wiedzieć, jak postąpić w przypadku wykrycia incydentu. Procedury Bezpiecznej Eksploatacji wraz ze Szczegółowymi Wymaganiami Bezpieczeństwa powinny opisywać zasady konfigurowania kont użytkowników, stosowane środki ochrony kryptograficznej oraz wymienione incydenty w bezpieczeństwie informacji. Ten fragment dokumentacji powinien być niejawny, gdyż adresowany jest do administratora. W grupie dokumentów, systemu bezpieczeństwa informacji, powinien znaleźć się plan przywracania systemu do działania po wystąpieniu awarii. Ważnym elementem w pracach nad dokumentacją jest przeprowadzenie analizy ryzyka bazującej na obserwacji systemu teleinformatycznego.

Wymienione dokumenty autor zaleca opracować centralnie na potrzeby Wojsk Lądowych. Zalecenie to powinno przynieść następujące korzyści:

- jednolite zasady konfiguracji elementów sieci, serwerów i stacji roboczych,
- jednolite miary pozwalające na ocenę poziomu bezpieczeństwa systemu teleinformatycznego,
- możliwość zatrudnienia specjalistów z dziedziny bezpieczeństwa teleinformatycznego wspomagających prace zespołu (np. przedstawiciele firm dostarczających oprogramowanie wykorzystane w systemie),
- jednolity program szkoleń dla użytkowników i administratorów teleinformatycznego systemu wspomagającego proces dowodzenia,
- przyjęcie jednolitego systemu przygotowania i przechowywania sprzętu potrzebnego do przywrócenia systemu do działania,
- uniknięcie problemów wynikających z różnic w poziomie wiedzy i umiejętności technicznych u administratorów LSK,
- możliwość zbierania informacji o występowaniu incydentów w bezpieczeń-

[14] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 43.

stwie teleinformatycznym w Wojskach Lądowych,

- przygotowanie procedur przywracania do działania oraz procedur prewencyjnych ograniczających liczbę incydentów w bezpieczeństwie informacji.

Proponowane rozwiązanie posiada wady, do których należą:

- duża inercja w działaniu instytucji wynikająca z obróbki dużej liczby danych dotyczących incydentów w bezpieczeństwie teleinformatycznym,
- problemy w dystrybucji opracowanych materiałów – różne systemy wsparcia dowodzenia i różne podatności,
- brak stałej kontroli nad procesem wdrażania procedur w podległych jednostkach,
- próby ukrywania części incydentów powstałych w wyniku niepoprawnej konfiguracji sprzętu lub oprogramowania.

Podsumowując liczba zalet scentralizowanego zarządzania dokumentacją bezpieczeństwa, w opinii autora, przewyższa liczbę wad. Podobne rozwiązanie funkcjonuje w Siłach Powietrznych, gdzie analizą sprawności technicznej statków powietrznych oraz dedukcyjnym dochodzeniem przyczyn niesprawności zajmuje się Instytut Techniczny Wojsk Lotniczych. Autor uważa, że doświadczenia Instytutu ze współpracy z jednostkami wojskowymi uda się zaadaptować do potrzeb sprawnej wymiany informacji w relacji jednostka wojskowa zespół analizy incydentów w bezpieczeństwie teleinformatycznym. Posiadanie sieci teleinformatycznych (np. Inter-MON) pozwala na szybką dystrybucję informacji do i z zespołu analizy incydentów teleinformatycznych. Problemem, jaki w opinii autora może powodować najwięcej zakłóceń w sprawnej wymianie informacji, jest brak świadomości wśród uczestników przedsięwzięcia o wadze zadań przez nich realizowanych. Niwelacja opisanego problemu będzie wymagała szkoleń pokazujących, że system wspomagania procesu dowodzenia traktowany jest – przez przełożonych i decydentów - jako całość, a nie jako wybrane fragmenty wdrożone i eksploatowane w jednostkach.

LITERATURA

1. Anderson R., *Inżynieria zabezpieczeń*, WNT, Warszawa 2005.
2. Białas A., *Bezpieczeństwo informacji i usług we współczesnej firmie i instytucji*, WNT, Warszawa 2007.
3. Jóźwiak I., J., Laskowski W., *Statistical Analysis of Security Attributes of Computer Systems*, [w:] International Journal of Reliability, Quality and Safety Engineering, Special Issue on SSARS 2007, Vol. 14, Number 6, December 2007, s. 569-577.
4. Jóźwiak I., J., Laskowski W., Szleszyński A., *Wykorzystanie techniki drzewa użyteczności w procesie planowania systemu bezpieczeństwa informacji*, Konferencja naukowa Strategie 2007, Podejmowanie decyzji w konfliktu i współpracy, Politechnika Śląska, [w przygotowaniu].
5. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.

6. Liderman K., *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?*, [w:] Biuletyn IAR nr 21/2004, Warszawa 2004, WAT, s.77-103.
7. Michniak J., *Dowodzenie i łączność*, AON, Warszawa 2005.
8. *International Standard ISO/IEC-15408-1. Information Technology – Security techniques – Evaluation criteria for IT security – Part 1*: Introduction and general model, Second edition 2005-10-01.
9. *Symatec Internet Security Threat Report*. Vol. XIII, [online]. [dostęp:2008] Dostępny w internecie: http: /www.symatec.com./.
10. *Ustawa z dnia 22.01.1999 „O ochronie informacji niejawnych"*, Dz.U. Nr 11 poz. 95 z późniejszymi zmianami.

Artykuł recenzował: dr inż. Leszek WOLANIUK