Cyberbezpieczeństwo systemów uzbrojenia sił powietrznych Stanów Zjednoczonych - zapewnienie bezpieczeństwa misji

Cybersecurity of United States Air Force Weapons Systems - ensuring mission security

Leszek Cwojdziński

Dr hab. inż. pil.

Airbus Poland S.A.

samolot221@wp.pl

Streszczenie: W niniejszym artykule zaprezentowano założenia dotyczące zagrożenia systemów uzbrojenia sił powietrznych które obecnie są w znacznym stopniu uzależnione od skomplikowanego oprogramowania i dużej ilości wzajemnych powiązań w celu realizacji misji bojowych. Zdolności cybernetyczne umożliwiają wiele zaawansowanych funkcji (np. atak elektroniczny, połączenie czujników i ich wzajemnej komunikacji), które dają lotnictwu bojowemu przewagę nad potencjalnymi przeciwnikami. Jednakże stanowią one również potencjalne możliwości i bodźce dla przeciwników do przeciwdziałania przewadze sił powietrznych poprzez ataki cybernetyczne. Autor omówił w jaki sposób wyrafinowany przeciwnik może dążyć do odkrycia i wykorzystania luk w oprogramowaniu samolotu, systemach wspomagających lub łańcuchu dostaw w celu zdobycia informacji wywiadowczych lub sabotowania operacji. Potencjalne ryzyko nie ogranicza się wyłącznie do najnowszych i najbardziej zaawansowanych system ale także do systemów które w ciągu najbliższej dekady lub dwóch będą wycofywane z eksploatacji. Starsze samoloty, które obecnie jeszcze stanowią większość zasobów US Air Force, są również narażone na ataki ze strony ewoluujących zagrożeń cybernetycznych i muszą podlegać ochronie. Audyty cyberbezpieczeństwa wykazują iż obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości dzisiejszego środowiska bezpieczeństwa cybernetycznego. Modelowa polityka bezpieczeństwa cybernetycznego ma służyć jako przewodnik pomagający państwom i ich siłom zbrojnym skupić zasoby i działania mające na celu osiągnięcie systemowego podejścia do cyberbezpieczeństwa w tym do obecnych i wprowadzanych w przyszłości systemów bojowych. Autor wskazuje iż celem tworzenia nowych rozwiązań jest, wypracowanie takiego rozwiązania, aby państwa oraz zainteresowane strony były w stanie opracować podejście typu system systemów (system-of-systems), które umożliwi ochronę przed zagrożeniami cybernetycznymi oraz reagowanie na incydenty cybernetyczne i usuwanie ich skutków w odpowiednim czasie, a tym samym zwiększenie odporności na nowe zagrożenia bez znaczących zakłóceń użycia systemów walki.

Słowa kluczowe: *Cyberbezpieczeństwo; Środowisko bezpieczeństwa; System systemów; Polityka bezpieczeństwa; Kultura bezpieczeństwa; Siły powietrzne; Lotnictwo bojowe; Systemy walki*

Abstract: This article presents assumptions about the threat to air force weapon systems which today are heavily dependent on complex software and a large number of interconnections to accomplish combat missions. Cyber capabilities enable many advanced functions (e.g., electronic attack, sensor interconnection and communications) that give combat aviation an advantage over potential adversaries. However, they also create potential opportunities and incentives for adversaries to counter the air force's superiority through cyber attacks. The author discusses how a sophisticated adversary may seek to discover and exploit vulnerabilities in aircraft software, support systems or the supply chain to gain intelligence or sabotage operations. The potential risk is not just limited to the newest and most advanced systems but also to systems that will be going out of service within the next decade or two. Older aircraft, which currently still make up the majority of US Air Force assets, are also vulnerable to attack from evolving cyber threats and must be protected. Cyber security audits show that current policies are better suited to simple, stable and predictable environments than to the complex, rapidly changing and unpredictable reality of today's cyber security environment. The model cybersecurity policy is intended to serve as a guide to help countries and their armed forces focus resources and activities to achieve a systemic approach to cyber security, including current and future combat systems being introduced. The author points out that the goal of developing new solutions is for states and stakeholders to be able to develop a systems-of-systems approach to protect against cyber threats and respond to and recover from cyber incidents in a timely manner, thereby increasing resilience to new threats without significant disruption to the use of combat systems.

Keywords: *Cyber security; Security environment; System of systems; Security policy; Security culture; Air force; Combat aviation; Combat systems*

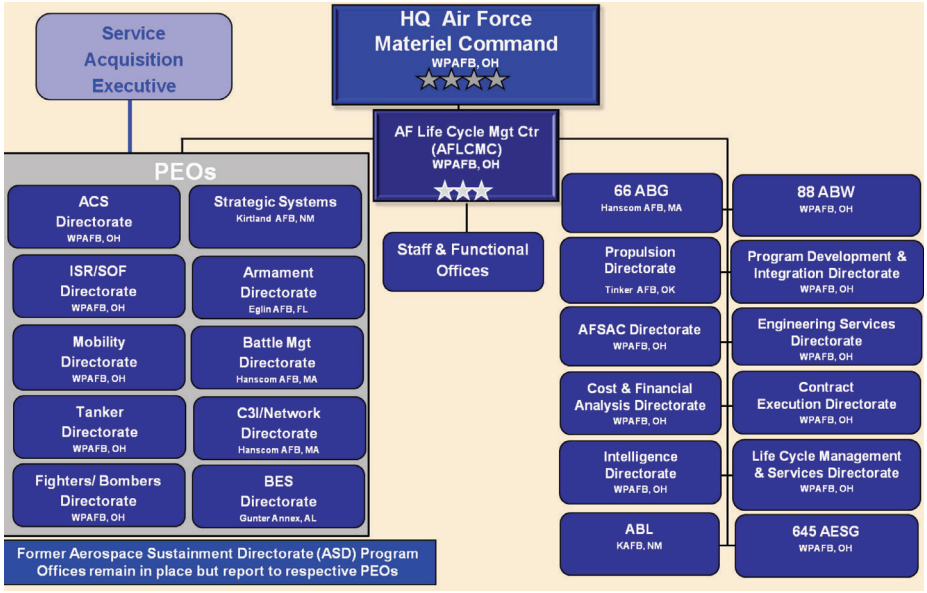
Systemy uzbrojenia Sił Powietrznych są dziś w znacznym stopniu uzależnione od skomplikowanego oprogramowania i dużej ilości wzajemnych połączeń w celu realizacji swoich misji. Zdolności cybernetyczne umożliwiają wiele zaawansowanych funkcji (np. atak elektroniczny, połączenie czujników i ich wzajemna komunikacja), które dają Siłom Powietrznym przewagę nad potencjalnymi przeciwnikami. Jednakże stwarzają one również potencjalne możliwości i bodźce dla przeciwników do przeciwdziałania przewadze USA poprzez ataki cybernetyczne. Przykładem jest wyrafinowany przeciwnik mogący dążyć do odkrycia i wykorzystania luk w oprogramowaniu samolotu, systemach wspomagających lub łańcuchu dostaw, w celu zdobycia informacji wywiadowczych lub sabotowania operacji. Potencjalne ryzyko nie ogranicza się wyłącznie do najnowszych

i najbardziej zaawansowanych systemów: Starsze samoloty, które obecnie jeszcze stanowią większość zapasów US Air Force, są również narażone na ataki ze strony ewoluujących zagrożeń cybernetycznych i muszą zachować czujność.

Aby zarządzać bezpieczeństwem cybernetycznym tych systemów, US Air Force i Departament Obrony USA (DoD ang. Department of Defence, Departament Obrony USA) potrzebują odpowiednich polityk wspierających projekty systemów, które są solidne i odporne na ataki cybernetyczne, projektów organizacyjnych, które są optymalnie ukształtowane, aby wdrożyć te polityki, oraz mechanizmów monitorowania i informacji zwrotnej, które uchwycą prawdziwy stan bezpieczeństwa cybernetycznego (w przeciwieństwie do zwykłej zgodności z obowiązującymi politykami) w całym cyklu eksploatacji systemu broni. Departament Obrony USA zaleca opracowanie modelowej polityki bezpieczeństwa cybernetycznego, do której państwa członkowskie NATO i przedstawiciele branży zbrojeniowej będą mogły się odwoływać przy opracowywaniu własnych polityk krajowych/wewnętrznych. Jedną z kluczowych organizacji powołanych do wsparcia eksploatacji systemów uzbrojenia Sił Powietrznych Stanów Zjednoczonych w pełnym cyklu eksploatacji jest The Air Force Life Cycle Management Center (AFLCMC) Centrum Zarządzania Cyklem Życia Sił Powietrznych z siedzibą w Wright-Patterson AFB. Stanowi ono jedno z sześciu ośrodków podlegających Dowództwu Sił Powietrznych, odpowiedzialnych za zarządzanie cyklem życia systemów uzbrojenia Sił Powietrznych USA od ich powstania do wycofania z eksploatacji. Misją AFLCMC jest wspieranie tych cech uzbrojenia które dzięki technicznej i technologicznej przewadze przechylą szalę zwycięstwa w konfliktach zbrojnych na stronę USA.

AFLCMC zostało zaprojektowane, aby zarządzać systemami uzbrojenia w całym cyklu eksploatacji oraz uprościć i skonsolidować funkcje i procesy personelu w celu ograniczenia redundancji i zwiększenia wydajności. Ponadto struktura operacyjna AFLCMC (rys.1.) zapewnia odpowiednie ramy dla podejmowania decyzji i optymalizacji procesów w całym cyklu życia systemu uzbrojenia. Personel AFLCMC ściśle współpracuje ze swoimi odpowiednikami w pozostałych ośrodkach obejmując nadzorem: systemy i sieci informatyczne; systemy dowodzenia, kontroli, łączności, wywiadu, obserwacji i rozpoznania; uzbrojenia; systemy strategiczne; platformy lotnicze oraz różne systemy specjalistyczne lub wspierające, takie jak np. symulatory i wyposażenie osobiste. AFLCMC realizuje również sprzedaż samolotów i innego sprzętu związanego z obronnością, budując jednocześnie relacje pomocy w zakresie bezpieczeństwa z siłami powietrznymi krajów partnerskich. Zadania te realizuje około dwadzieścia sześć tysięcy specjalistów Sił Powietrznych AFLCMC, pracowników cywilnych i wykonawców centrum z dziewięciu głównych lokalizacji i kilkudziesięciu mniejszych. Dowódca AFLCMC jest odpowiedzialny za organizację, szkolenie i wyposażenie centrum, w tym procesy zarządzania cyklem życia. Każde Biuro Programowe podlega jednemu z 10 Oficerów Wykonawczych Programu (PEO ang. Program Executive Director, Oficer Wykonawczy Programu), którzy są odpowiedzialni za działania w ramach swojego zakresu odpowiedzialności i podlegają Air Force Service Acquisition Executive w Pentagonie (Assistant Secretary of the Air Force for Acquisition). Dyrekcja Wsparcia Bezpieczeństwa i Współpracy Sił Powietrznych nadzoruje realizację misji zagranicznej sprzedaży wojskowej. Dyrekcja Napędów nadzoruje pozyskiwanie silników i wsparcie produktowe. Dyrekcje wsparcia AFLCMC zapewniają bezpośrednie wsparcie programowe, takie jak inżynieria, zarządzanie zamówieniami technicznymi, planowanie rozwoju, kontraktowanie i pomoc w wyborze źródeł dostaw. Dyrekcje wsparcia obejmują: Program Execution; Technical Engineering Services; Financial Management Mission; Logistics Services; Contract Execution; Cyber & Analysis Programs; Program Development & Integration oraz Intelligence.

Centrum Zarządzania Cyklem Życia US Air Force zwróciło się do RAND Project AIR FORCE (PAF) z prośbą o ocenę obecnych przepisów, polityk, organizacji i procesów pod kątem najlepszych praktyk i solidnych zasad cyberbezpieczeństwa oraz o zarekomendowanie kroków w celu poprawy. Badania skupiły się na systemach



***1**. Struktura organizacyjna AFLCMC. Źródło:https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383*

bezpieczeństwa narodowego, dla których Siły Powietrzne mają pewną kontrolę nad projektami, architekturami, protokołami i interfejsami, w przeciwieństwie do komercyjnych, gotowych systemów informatycznych i biznesowych (COTS ang. Commercial Off-The-Shelf – prosto z półki). Misją PAF jest prowadzenie zintegrowanego programu obiektywnych analiz w kwestiach będących przedmiotem trwałego zainteresowania Departamentu Sił Powietrznych. PAF zajmuje się dalekosiężnymi i wzajemnie powiązanymi pytaniami: Jaka będzie rola sił powietrznych i kosmicznych w przyszłym środowisku bezpieczeństwa? Jak należy modernizować siły, aby sprostać zmieniającym się wymaganiom operacyjnym? Jaka powinna być wielkość i charakterystyka pracowników departamentu i jak można ją najskuteczniej rekrutować, wyszkolić i zatrzymać w służbie? Jak należy usprawnić utrzymanie i pozyskiwanie infrastruktury, aby kontrolować koszty?

PAF pierwotnie znany jako Projekt RAND (– nazwa RAND jest skrótem od Research ANd Development (badania i rozwój), został założony w 1946 roku przez generała H. H. "Hap" Arnolda jako sposób na zachowanie znacznych korzyści płynących z cywilnej myśli naukowej, które zostały zademonstrowane podczas II wojny światowej. Od momentu powstania, PAF pozostaje jedynym finansowanym przez Departament Sił Powietrznych centrum badawczo-rozwojowym (FFRDC - Federally Financed Research And Development Center) zajmującym się wyłącznie badaniami i analizami, a nie inżynierią systemów czy laboratoriami naukowymi. Specjalny status FFRDC ułatwia stabilne wsparcie Departamentu Sił Powietrznych przez dłuższy okres czasu, jak również dostęp personelu badawczego do odpowiednich informacji Departamentu i personelu zarządzającego. Zapotrzebowanie Departamentu Sił Powietrznych na wsparcie analityczne ze strony PAF doprowadziło do ustanowienia czterech programów badawczych reprezentujących podstawowe możliwości:

- STRATEGIA I DOKTRYNA dąży do zwiększenia wiedzy i zrozumienia problemów geopolitycznych i innych problemów w środowiskach bezpieczeństwa narodowego, które mają wpływ na operacje Departamentu Sił Powietrznych. PAF wykonuje ekspertyzy w zakresie wielkiej strategii; ewoluujących wyzwań bezpieczeństwa; projekcji siły; operacji ekspedycyjnych; oraz zmieniających się ról sił powietrznych, kosmicznych i cybernetycznych w obecnych i przyszłych operacjach.
- MODERNIZACJA I ROZWÓJ SIŁ LĄDOWYCH identyfikuje i ocenia sposoby, w jakie postęp technologiczny i nowe koncepcje operacyjne mogą poprawić zdolność Departamentu Sił Powietrznych do zaspokojenia szeregu przyszłych wymagań operacyjnych. Badania te obejmują ocenę wykonalności technologii, wydajności, kosztów i ryzyka. PAF ocenia główne komponenty sił powietrznych, kosmicznych i cybernetycznych potrzebne w przyszłości oraz systemy i infrastrukturę wspierające ich działanie. Obszary specjalizacji obejmują wywiad, nadzór, rozpoznanie, mobilność, uderzenie dalekiego zasięgu, bojowe siły powietrzne, dowodzenie i kontrolę, przestrzeń kosmiczną, cybernetyczną i nuklearną.
- RESOURCE MANAGEMENT analizuje polityki i praktyki w ramach trzech tematów: (1) odporności instalacji DAF (ang. Detect-A-Fire, instalacja wykrywania pożaru), aktywów i informacji, (2) skutecznej i efektywnej alokacji zasobów oraz, (3) zdrowia bazy przemysłowej i technologicznej obrony. Celem badań prowadzonych w ramach programu jest maksymalizacja skuteczności i efektywności operacji w środowisku o ograniczonych zasobach.

WORKFORCE, DEVELOPMENT, AND HEALTH (dawniej Manpower, Personnel, and Training) bada wielkość i skład personelu Departamentu Sił Powietrznych oraz zajmuje się najlepszymi sposobami definiowania, podtrzymywania, odnawiania, dostarczania i koordynowania krytycznych zdolności roboczych. PAF rozważa również rozwój personelu, taki jak szkolenia, możliwości zatrudnienia i awansu zawodowego, a także analizuje zdrowie fizyczne i psychiczne pracowników. Badania PAF obejmują całą siłę roboczą: aktywną służbę, gwardię, rezerwę, personel cywilny i wykonawczy. PAF prowadzi również szeroko zakrojone badania na tematy, które dotyczą wszystkich czterech programów, a także regularnie odpowiada na prośby Sił Powietrznych o pomoc w rozwiązaniu pilnych problemów.

Spostrzeżenia dotyczące zarządzania bezpieczeństwem cybernetycznym.

Eksperci PAF wyszli z założenia, że pożądanymi rezultatami zarządzania bezpieczeństwem cybernetycznym jest (1) ograniczenie ilości informacji krytycznych, które może uzyskać przeciwnik w wyniku udanej eksfiltracji oraz (2) utrzymanie akceptowalnego poziomu funkcjonalności operacyjnej nawet w przypadku ataku. Wyniki te muszą być osiągane w sposób ciągły przez cały cykl życia systemu wojskowego, od badań i rozwoju do utylizacji. Wszystkie etapy są ważne, ale etapy rozwoju i utrzymania są szczególnie krytyczne: pierwszy z nich wynika z podejmowania decyzji projektowych, które mogą ograniczyć możliwości w przyszłości, a drugi z faktu, że większość systemów pozostaje w stanie utrzymania przez większość cyklu życia. Biorąc pod uwagę te cele w zakresie bezpieczeństwa cybernetycznego, przegląd literatury

ujawnia dwie obserwacje dotyczące projektu organizacyjnego i informacji zwrotnej w celu osiągnięcia tych celów w zakresie bezpieczeństwa cybernetycznego.

Projekt organizacyjny powinien być elastyczny i zdecentralizowany. Środowisko cyberbezpieczeństwa jest z natury dynamiczne i złożone. Literatura sugeruje, że dobrze zarządzane organizacje radzą sobie z takim środowiskiem wybierając projekty organizacyjne, które faworyzują rozwiązania uzyskane poprzez zdecentralizowaną koordynację i współpracę pracowników nad rozwiązaniami zalecanymi przez standardowe i sformalizowane kontrole. Informacje zwrotne oparte na wynikach są bardziej wartościowe niż informacje zwrotne oparte na zgodności. Organizacje mają tendencję do skupiania się na łatwo obserwowalnych wskaźnikach, takich jak zgodność z politykami i dyrektywami, aby wskazać swój poziom bezpieczeństwa cybernetycznego. Jednak zgodność sama w sobie nie odzwierciedla rzeczywistego stanu bezpieczeństwa cybernetycznego, zwłaszcza w złożonych i szybko zmieniających się środowiskach zagrożeń. Organizacje powinny raczej skupić się na tym, czy ich polityka i praktyki osiągają pożądane rezultaty (np. zapewnienie misji w obliczu adaptacyjnych cyberataków) i powinny być gotowe do dostosowania się w razie potrzeby.

Obecne braki i ich implikacje

Porównanie tych zasad zarządzania ze szczegółowym przeglądem przepisów i polityk regulujących cyberbezpieczeństwo w US Air Force ujawnia szereg luk. Obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości środowiska bezpieczeństwa cybernetycznego. Departament Obrony USA dąży do standaryzacji bezpieczeństwa cybernetycznego poprzez zastosowanie kontroli bezpieczeństwa Narodowego Instytutu Standardów i Technologii (NIST) do wszystkich systemów, w tym systemów uzbrojenia. Kontrole te mają na celu złagodzenie problemów bezpieczeństwa w projektach, które Siły Powietrzne dziedziczą, takich jak systemy COTS. Z kolei systemy uzbrojenia dają projektantom możliwość budowania systemów, które są bardziej bezpieczne z natury. Solidna inżynieria bezpieczeństwa systemu na wczesnym etapie projektowania systemu broni byłaby bardziej skuteczna niż kontrole bezpieczeństwa, które są stosowane jako nakładki na projekty stworzone bez cyberbezpieczeństwa jako integralnego priorytetu. Bezpieczeństwo cybernetyczne opiera się na danych wywiadowczych, zagrożeniach i zarządzaniu ryzykiem, które stanowi integralną część całego cyklu życia systemów. Wszystkie dane i systemy muszą mieć przez cały czas ustalonego właściciela. Funkcje, systemu i infrastruktura o znaczeniu krytycznym są identyfikowane w ramach procesów zarządzania ryzykiem. Do ochrony systemów krytycznych stosuje się podejście "security by design" w połączeniu z zasadami "Defence in depth". Redundancja systemów krytycznych jest traktowana jako czynnik zwiększający bezpieczeństwo systemu. Dane i informacje są chronione podczas przechowywania i przekazywania, zgodnie z ich wrażliwościami. Zarządzanie całym łańcuchem dostaw oprogramowania/sprzętu komputerowego stanowi część zarządzania bezpieczeństwem cybernetycznym lotnictwa. Oprogramowanie i sprzęt wykorzystywany w krytycznych funkcjach lotnictwa muszą spełniać wymogi w zakresie bezpieczeństwa cybernetycznego przez cały cykl życia bojowych systemów lotniczych. Ochrona fizyczna (w tym ochrona personelu) jest częścią zarządzania cyberbezpieczeństwem w lotnictwie. Zadaniem ochrony fizycznej jest zabezpieczenie ludzi, infrastruktury, obiektów, sprzętu, materiałów i dokumentów przed bezprawną ingerencją oraz ochrona krytycznych systemów lotniczych przed nieuprawnionym dostępem fizycznym. Ochrona fizyczna przyczynia się do zarządzania ryzykiem poprzez identyfikację podmiotów stanowiących zagrożenie i/lub prawdopodobieństwo ataków na krytyczną infrastrukturę lotnictwa wojskowego. Ochrona informacji, komunikacji i technologii (ICT) jest częścią zarządzania cyberbezpieczeństwem lotnictwa, określa i wdraża logiczne środki bezpieczeństwa, a także przyczynia się do zarządzania incydentami cybernetycznymi, odzyskiwania danych i ciągłości działania w procesach zarządzania incydentami cybernetycznymi, odzyskiwania danych i ciągłości działania. Bezpieczeństwo teleinformatyczne przyczynia się do zarządzania ryzykiem poprzez identyfikację podatności, obszarów i kierunków ataku oraz monitorowanie zmian w krajobrazie zagrożeń dla bezpieczeństwa cybernetycznego. Zarządzanie incydentami i ciągłość funkcji krytycznych są głównymi czynnikami w procesach zarządzania incydentami. Nieodłącznym procesem jest testowanie planów zarządzania kryzysowego i odzyskiwania danych, które stanowi integralną część zarządzania incydentami.

Wdrażanie bezpieczeństwa cybernetycznego nie jest stale aktywne przez cały cykl życia systemu wojskowego. Zwrócenie uwagi na bezpieczeństwo cybernetyczne jest zazwyczaj wywoływane przez wydarzenia związane z pozyskiwaniem uzbrojenia, które najczęściej mają miejsce podczas zamówień publicznych. W rezultacie polityka nie obejmuje pełnego zakresu kwestii związanych z bezpieczeństwem cybernetycznym, które mają wpływ na system w całym jego cyklu życia. Ten brak ma kilka istotnych konsekwencji. Po pierwsze, programowe czynniki wyzwalające w zakresie bezpieczeństwa cybernetycznego pojawiają się na późnym etapie procesu projektowania i w

związku z tym mają niewielki wpływ na kluczowe decyzje projektowe, które mają wpływ na bezpieczeństwo cybernetyczne. Po drugie, systemom w programach znajdujących się poza fazą zamówień publicznych (tj. w fazie podtrzymywania lub likwidacji) poświęca się mniej uwagi niż systemom w fazie zamówień publicznych. Jak wspomniano powyżej, powoduje to niedocenianie większości systemów US Air Force, które są w fazie konserwacji. Po trzecie, ta struktura polityki ma tendencję do faworyzowania ocen podatności (przeważających w fazie projektowania) nad ocenami wpływu misji i zagrożeń (które mają wpływ na cały cykl życia). Wreszcie, zarządzanie, nadzór i budżetowanie w ramach Departamentu Obrony Stanów Zjednoczonych są silnie ustrukturyzowane wokół programów, podczas gdy podatności w zakresie bezpieczeństwa cybernetycznego przekraczają granice programów. Powoduje to rozbieżność między wyzwaniami w zakresie bezpieczeństwa cybernetycznego w poszczególnych systemach a sposobem zarządzania nimi.

Monitorowanie i informacje zwrotne dotyczące bezpieczeństwa cybernetycznego są niepełne, nieskoordynowane i niewystarczające do skutecznego podejmowania decyzji lub odpowiedzialności. Obecne informacje zwrotne nie obejmują wszystkich systemów, nie badają konsekwencji braków w zakresie bezpieczeństwa cybernetycznego i nie są przekazywane w formie umożliwiającej podejmowanie skutecznych decyzji. Brak kompleksowych, zorientowanych na program lub system informacji zwrotnych na temat bezpieczeństwa cybernetycznego oraz wpływu bezpieczeństwa cybernetycznego na misje operacyjne kontrastuje z dużą ilością informacji zwrotnych na temat kosztów i harmonogramu. Ta nierównowaga stwarza strukturę motywacyjną dla kierowników programów i dyrektorów wykonawczych programów, którzy przedkładają koszty i harmonogram nad wyniki w zakresie bezpieczeństwa cybernetycznego. Te braki w informacjach zwrotnych dotyczących bezpieczeństwa cybernetycznego dodatkowo ograniczają indywidualną odpowiedzialność.

Zalecenia mające na celu usunięcie niedociągnięć

Żadne proste rozwiązanie nie skoryguje wszystkich powyższych braków, z których wiele jest strukturalnie zakorzenionych w Departamencie Obrony USA. Niektóre wynikają z dobrze pomyślanych wymogów ustawowych i polityk Departamentu Obrony, które niełatwo zmienić. Jednakże, w ramach tych ograniczeń, istnieją kroki, które Siły Powietrzne mogą podjąć w celu wzmocnienia bezpieczeństwa cybernetycznego systemów uzbrojenia:

- Zdefiniowanie celów cyberbezpieczeństwa dla systemów wojskowych w Siłach Powietrznych wokół pożądanych wyników, pozostając jednocześnie w zgodzie z wytycznymi Departamentu Obrony. Cel roboczy stanowi utrzymanie wpływu wykorzystania cybernetycznego i ofensywnych operacji cybernetycznych przeciwnika na akceptowalnym poziomie, zgodnie ze standardowym procesem oceny ryzyka dla zapewnienia misji.
- Przeformułowanie ról i obowiązków funkcjonalnych w zakresie oceny ryzyka związanego z bezpieczeństwem cybernetycznym w oparciu o równowagę między podatnością systemu, zagrożeniem i wpływem na misję operacyjną, a także nadać urzędnikowi zatwierdzającemu uprawnienia do integracji i rozstrzygania między zainteresowanymi stronami. Na przykład społeczność zarządzająca cyklem życia (w szczególności kierownik programu) byłaby odpowiedzialna za oceny podatności programu i systemu, społeczności wywiadowcze i kontrwywiadowcze byłyby odpowiedzialne za oceny zagrożeń, a właściciel misji (np. główny integrator funkcji podstawowych, główne dowództwo) byłby odpowiedzialny za oceny zapewnienia misji operacyjnej. Urzędnik zatwierdzający integruje i równoważy te punkty widzenia w oparciu o akceptowalny poziom ryzyka cyberbezpieczeństwa.
- Przydzielenie każdemu urzędnikowi zatwierdzającemu portfela systemów i zapewnienie, że wszystkie systemy wyraźnie podlegają jakiemuś urzędnikowi zatwierdzającemu przez cały cykl życia.
- Zachęcanie biur programowych US Air Force do uzupełnienia wymaganych kontroli bezpieczeństwa DoD (które koncentrują się na likwidowaniu słabych punktów) o bardziej kompleksowe środki bezpieczeństwa cybernetycznego, w tym solidną inżynierię bezpieczeństwa systemu (która koncentruje się na zapewnieniu solidności i odporności systemu w obliczu udanych ataków).
- Wspieranie innowacji i adaptacji w zakresie bezpieczeństwa cybernetycznego poprzez decentralizację, w ramach każdej nowej polityki US Air Force, sposobu wdrażania inżynierii bezpieczeństwa systemu w ramach poszczególnych programów.
- Ocenę kompromisów między ryzykiem związanym z bezpieczeństwem cybernetycznym a korzyściami funkcjonalnymi związanymi z łączeniem systemów wojskowych w cyberprzestrzeni. Celem jest odwrócenie domyślnej kultury łączenia systemów, gdy tylko jest to możliwe, i zmniejszyłoby złożoność bezpieczeństwa cybernetycznego.
- Stworzenie grupy ekspertów w dziedzinie bezpieczeństwa cybernetycznego, którzy mogą

być w razie potrzeby łączeni w ramach społeczności cyklu życia, udostępniając zasoby małym programom i programom w fazie podtrzymywania.

- Ustanowienie priorytetów dla przedsiębiorstw w zakresie oceny i rozwiązywania problemów bezpieczeństwa cybernetycznego w starszych systemach.
- Zlikwidowanie luk w informacjach zwrotnych i zwiększenie widoczności cyberbezpieczeństwa poprzez sporządzanie regularnej, ciągłej oceny podsumowującej stan cyberbezpieczeństwa dla każdego programu w US Air Force. Pociągnąć kierowników programów do odpowiedzialności za reakcję na problemy.
- Stworzenie czerwonych zespołów ds. cyberbezpieczeństwa, które są dedykowane do zarządzania nabyciem/cyklem życia w US Air Force.
- Pociągnięcie osób do odpowiedzialności za umyślne naruszenie zasad cyberbezpieczeństwa.
- Opracowanie danych dotyczących zagrożeń misji w celu wsparcia kierowników programów i urzędników zatwierdzających w ocenie akceptowalnego ryzyka dla misji spowodowanego brakami w zakresie bezpieczeństwa cybernetycznego w systemach i programach.

Należy zdawać sobie sprawę, iż zalecenia te, nawet jeśli zostaną w pełni wdrożone, nie rozwiążą całkowicie problemów związanych z bezpieczeństwem cybernetycznym. Co więcej, niektóre z tych polityk wymagałyby dodatkowych zasobów i odpowiednio wykwalifikowanej siły roboczej do realizacji obowiązków - zobowiązań, które są trudne do podjęcia w ograniczonym środowisku fiskalnym. Faktem jest, że nie ma szybkich ani łatwych rozwiązań pozwalających osiągnąć światowej klasy bezpieczeństwo cybernetyczne. Jednak przyjmując te zalecenia, Siły Powietrzne zrobiłyby duży krok w kierunku skuteczniejszego zabezpieczenia cybernetycznego swoich systemów wojskowych w całym cyklu ich życia. Kultura bezpieczeństwa cybernetycznego jest bardzo ważnym elementem polityki bezpieczeństwa. Opracowany dla jej wdrażania plan edukacji, świadomości, szkoleń i ćwiczeń stanowi integralną część zarządzania bezpieczeństwem cybernetycznym systemów uzbrojenia sił powietrznych. Kultura bezpieczeństwa cybernetycznego jest w pełni skoordynowana z istniejącymi kulturami bezpieczeństwa i ochrony, wspierają ją solidne wewnętrzne i w miarę możliwości, zewnętrzne praktyki wymiany informacji.

Główne wnioski

Audyty cyberbezpieczeństwa wykazują iż obecne polityki są lepiej dostosowane do prostych, stabilnych i przewidywalnych środowisk niż do złożonej, szybko zmieniającej się i nieprzewidywalnej rzeczywistości środowiska bezpieczeństwa cybernetycznego.

- Wdrożenie bezpieczeństwa cybernetycznego nie jest stale utrzymywane na odpowiednim poziomie przez cały cykl życia systemu wojskowego.
- Kontrola i odpowiedzialność za bezpieczeństwo cybernetyczne systemów wojskowych jest rozłożona na wiele organizacji i słabo zintegrowana.
- Monitorowanie i informacje zwrotne dotyczące cyberbezpieczeństwa są niekompletne, nieskoordynowane i niewystarczające do skutecznego podejmowania decyzji lub odpowiedzialności struktur i osób funkcyjnych.

Modelowa polityka bezpieczeństwa cybernetycznego ma służyć jako przewodnik pomagający państwom i ich siłom zbrojnym skupić zasoby i działania mające na celu osiągnięcie systemowego podejścia do cyberbezpieczeństwa w US Air Force, w tym do obecnych i systemy dotychczasowe. Ostatecznym celem jest, aby państwa oraz zainteresowane strony były w stanie opracować podejście typu system systemów (system-of--systems), które umożliwi ochronę przed zagrożeniami cybernetycznymi oraz reagowanie na incydenty cybernetyczne i usuwanie ich skutków w odpowiednim czasie, a tym samym odporność na nowe zagrożenia bez znaczących zakłóceń.

Główne wyniki, jakich oczekuje się po wdrożeniu polityki bezpieczeństwa cybernetycznego to określenie ram dla dalszego rozwoju i wdrażania bezpieczeństwa cybernetycznego w Siłach Powietrznych. Będzie to realizowane dzięki publikowaniu i rozpowszechnianiu polityki bezpieczeństwa wśród właściwych zainteresowanych struktur i poddawaniu jej okresowym przeglądom.◀

Materiały źródłowe

[1] website belongs to an official U.S. Department of Defense organization in the United States.
[2] https://www.afsbirsttr.af.mil/About/Cybersecurity-and-the-Blue-Cyber-Education-Series/
[3] Official websites use .mil ., An official website of the United States government
[4] https://hii.com/wp-content/uploads/2023/03/HII-Game--Changer-9.1.22.pd
[5] https://www.hanscom.af.mil/Portals/57/documents/AFD-120716-005.pdf?ver=2016-07-11-082154-383
[6] https://nap.nationalacademies.org/read/25393/chapter/1
[7] https://www.aflcmc.af.mil/WELCOME/Organizations/
[8] https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf