JOURNAL OF MODERN SCIENCE
TOM 1/50/2023
www.jomswsge.com

DOI: https://doi.org/10.13166/jms/161536

Wojciech Wróblewski
The Main School of Fire Service in Warsaw, Poland
wwroblewski@sgsp.edu.pl
ORCID: 0000-0003-3415-9485

Norbert Tuśnio
The Main School of Fire Service in Warsaw, Poland
ntusnio@sgsp.edu.pl
ORCID: 0000-0003-0878-8499

REDUKCJA RYZYKA INCYDENTU W OPARCIU O ANALIZĘ RYZYKA W CYBERPRZESTRZENI OPERACYJNEJ STRAŻY POŻARNEJ. PERSPEKTYWA CYBERBEZPIECZEŃSTWA

INCIDENT RISK REDUCTION BASED ON RISK ANALYSIS IN THE OPERATIONAL CYBERSPACE OF THE FIRE BRIGADE. CYBERSECURITY PERSPECTIVE

Abstract

The purpose of the study was to analyze past cyber attacks on fire department operational sys-tems and to assess the risks of a cyber incident.

Analysis of data from open sources and bicriteria analysis of studies in scientific databases were used. A graphical method for assessing the level of risk using a two-dimensional matrix was also used.

The highest risk level of 15 was recorded for phishing attacks in Confidentiality and Availability of data, followed by ransomware attacks in the same area. In the area

of drone events in firefighting operations, the highest risk level of 6 was recorded for GPS Spoofing attacks during a mass event in terms of data availability (Availability).

To date, fire department cyber incidents have not affected business continuity. However, in the event of a mass or hybrid incident, the occurrence of an incident in operational systems, can signif-icantly reduce operational capacity and thus affect life-saving operations.

Streszczenie

Celem opracowania była analiza dotychczasowych cyberataków w systemach operacyjnych stra-ży pożarnej oraz oszacowanie ryzyk w związku z wystąpieniem incydentu w cyberprzestrzeni.

Wykorzystano analizę danych ze źródeł otwartych oraz dwukryterialną analizę opracowań w bazach naukowych. Wykorzystano również graficzną metodę oceny poziomu ryzyka za pomocą dwuwymiarowej macierzy.

Największy poziom ryzyka, wynoszący 15, odnotowano dla ataków phishing w zakresie poufno-ści (Confidentiality) i dostępności (Availability) danych, a następnie dla ataków ransomware w tym samym obszarze. W obszarze zdarzeń z wykorzystaniem dronów w działaniach operacyj-nych straży pożarnej największy poziom ryzyka, wynoszący 6, odnotowano dla ataku GPS Spoo-fing w czasie zdarzenia masowego w zakresie dostępności (Availability) danych.

Dotychczasowe incydenty w cyberprzestrzeni straży pożarnej nie wpłynęły na zachowanie cią-głości działania. Jednak w przypadku zdarzenia o charakterze masowym lub hybrydowym, wy-stąpienie incydentu w systemach operacyjnych, może znacząco obniżyć zdolność operacyjną a tym samym wpłynąć na działania ratujące życie.

Keywords: *security, risk management, cyber security, fire brigade, cybersecurity management*

Słowa kluczowe: *bezpieczeństwo, cyberbezpieczeństwo, zarządzanie ryzykiem, straż pożarna, zarządzanie cyber-bezpieczeństwem*

Wprowadzenie

Współczesne środowisko bezpieczeństwa charakteryzuje się zmianą paradygmatów wśród których istotną rolę odgrywają nowe technologie, wspierające zadania operacyjne wszystkich poziomów organizacji sektora publicznego.

Wdrożenia technologiczne to z jednej strony atrybut o koniecznym charakterze, jednak z drugiej strony obszar ten stanowi platformę wielu zagrożeń i ryzyk w cyberprzestrzeni. Materializowanie się cyberzagrożeń może prowadzić do katastrofalnych skutków, które coraz częściej mogą przybierać postać kaskadową. Przykładem mogą być cyberataki na infrastrukturę ochrony zdrowia w czasie pandemii SARS-CoV-2, które destabilizowały pracę oddziałów ratunkowych i laboratoriów, zagrażając życiu pacjentów (Maia i in., 2020, s. 142–165) czy też wojna hybrydowa w Ukrainie, gdzie cyberprzestrzeń została wykorzystana m.in. w procesach dezinformacji, co skutkowało np. opóźnioną reakcją ludności cywilnej na inne zagrożenia, w tym także kinetyczne. Problem ten opisuje szerzej Zegarow w raporcie NASK (Naukowa i Akademicka Sieć Komputerowa), stwierdzając, że *fałszywe wiadomości wywierają negatywny wpływ na emocje, rozumowanie i zachowanie człowieka poprzez kreowanie nieprawdziwego obrazu rzeczywistości* (Zegarow, 2019, s. 25–29). Cyberprzestrzeń stała się zatem ważnym elementem współczesnego środowiska bezpieczeństwa, generując przy tym konieczność szeregu działań pragmatycznych i formalno-organizacyjnych w wymiarze istniejących systemów bezpieczeństwa globalnego oraz lokalnego (Brooks i in., 2018, s. 10).

Jednym z kluczowych podmiotów realizujących zadania w obszarze bezpieczeństwa jest Państwowa Straż Pożarna (PSP), która – jako zawodowa, umundurowana oraz wyposażona w specjalistyczny sprzęt formacja – jest przeznaczona m.in. do walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami (Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej art. 1). Państwowa Straż Pożarna jako część składowa administracji działa w ramach podmiotów właściwych w sprawach ochrony bezpieczeństwa i porządku publicznego. Szeroki zakres działania straży pożarnej z tendencją do stałego poszerzania się w wyniku zmieniającej się rzeczywistości i zagrożeń, wiąże się z przypisanymi jej różnymi funkcjami i jest realizowany z uwzględnieniem prawnych form działania administracji (Liwo, 2020, s. 105–132). Zdecydowana większość operacyjnych procesów straży pożarnej została zintegrowana z sieciowo i organizacyjnie powiązanymi, strukturalnie zorganizowanymi technologiami (systemami) teleinformatycznymi. Należą do nich m.in.: system wspomagania decyzji (SWD), System DSP-50, Terminal statusów, Konsola TRX czy Geographic Information System (GIS) oraz coraz

częściej wykorzystywane w działaniach operacyjnych systemy bezzałogowych statków powietrznych (BSP). Wdrażanie nowych technologii w straży pożarnej usprawnia procesy operacyjne, ale jednocześnie stanowi przestrzeń podatności na cyberataki. Jak zauważono w *Protecting Against Cyberattacks: A Guide for Public Safety Leaders* niewielka podatność może spowodować znaczące szkody poprzez sparaliżowanie systemów teleinformatycznych, naruszyć przechowywanie danych w tym informacji poufnych oraz zagrozić zdolności operacyjnej, czego bezpośrednią konsekwencją może być narażenie ludzkiego życia (Cooper, s. 4–12).

Celem niniejszej publikacji jest analiza dotychczasowych incydentów w cyberprzestrzeni straży pożarnej oraz oszacowanie i zredukowanie ryzyka zaistnienia incydentów typu phishing i ransomware, a także powiązanych z wykorzystaniem bezzałogowych systemów powietrznych (GPS spoofing oraz down link intercept). Problem badawczy został ujęty w pytaniu: Czy incydenty w cyberprzestrzeni operacyjnej straży pożarnej mogą mieć wpływ na funkcjonowanie bazodanowych systemów wspomagania decyzji oraz czy w kontekście działań operacyjnych mogą utrudnić prawidłową lokalizację pożaru czy też przyczynić się do utraty danych pozyskanych na miejscu zdarzenia?

Metodologia

Realizacja przyjętego celu została oparta na kilku etapach. Przeprowadzono analizę baz naukowych (Google Scholar; Science Direct; Research Gate). W opracowaniu przyjęto kryterium czasu (lata 2021–2023) oraz zakresu (frazy: cyberbezpieczeństwo; straż pożarna). Analiza wykazała następujące rekordy: Google Scholar – 5370 rekordów, Science Direct – 876 rekordów oraz Research Gate – 1000 rekordów. W zindeksowanych opracowaniach nie poruszono bezpośrednio obszaru cyberbezpieczeństwa w straży pożarnej. Przeprowadzono analizę zdarzeń ze źródeł otwartych oraz raportów ENISA 2021 i CERT Polska 2021, które wykazały, że sektor publiczny był jednym z najczęściej atakowanych obszarów. Dokonano selekcji incydentów w cyberprzestrzeni a następnie wskazano ryzyka dla każdego z zagrożeń. Wykorzystano metodę matrycy ryzyka – graficzną metodę oceny poziomu

ryzyka za pomocą dwuwymiarowej macierzy, w której jedną zmienną jest prawdopodobieństwo wystąpienia zagrożenia, a drugą skutki tego zagrożenia. Ocena prawdopodobieństwa i skutków zdarzeń została przeprowadzona w skali pięciostopniowej. Po oszacowaniu parametrów ryzyka dokonano określenia poziomu ryzyka (w skali od 1 do 25). Wartości ryzyka zostały wykazane w dwustopniowym modelu, w którym przyjęto incydent w rutynowym środowisku operacyjnym oraz incydent w zdarzeniu masowym.

Rezultaty

Analiza źródeł otwartych wykazała, że w ostatnich latach doszło do ataków hakerskich w systemach operacyjnych straży pożarnej (głównie w Stanach Zjednoczonych). Według danych, na które powołuje się Firehouse, w styczniu 2014 r. naruszono bezpieczeństwo danych kilku jednostek straży pożarnej w hrabstwie King w stanie Waszyngton; w kwietniu 2015 r. straż pożarna w Salisbury (Massachusetts), padła ofiarą cyberataku; w listopadzie 2015 r. regionalne centrum dyspozytorskie w hrabstwie Strafford w stanie New Jersey zostało zaatakowane przez oprogramowanie ransomware; we wrześniu 2016 r. straż pożarna w Honolulu została zainfekowana wirusem ransomware; w kwietniu 2017 r. hakerzy włamali się i uruchomili system alarmowania w rejonie Dallas; w lipcu 2017 r. m.in. straż pożarna w Murfreesboro została zainfekowana w atakach oprogramowaniem ransomware Wanna Cry (Kosik, 2017, Oct. 14). Przeprowadzony 3 maja 2018 r. atak ransomware (drugi w ciągu trzech tygodni), spowodował utratę danych policji i straży pożarnej w Riverside. Atak zablokował poufne dane, w tym dane zawierające informacje o trwających dochodzeniach (Chevreaux i in., 2021, s. 19). W czerwcu 2019 r. zhakowano komputery straży pożarnej, zakłócając dyspozycję i potencjalnie narażając dane (Garbe, 2018). Ponadto w 2018 r. w Baltimore zhakowano system dyspozytorski 911, ograniczając znacznie jego funkcjonalności (Rector, 2018). W marcu 2020 r. w czasie trwania pandemii COVID-19 przy wykorzystaniu ransomware, zhakowano serwery komputerowe straży pożarnej w Bluffton Township Fire District. Skutkiem ataku były problemy z systemami ewidencjonowania zdarzeń (The Island Packet, 2021).

Według Administrative Hack Fire Department mamy do czynienia z wielowektorowym wskaźnikiem zagrożeń w cyberprzestrzeni, wśród których za najbardziej istotne dla straży pożarnej, można uznać oszustwa phishingowe i ataki ransomware. W ocenie Federal Trade Commision (FTC), phishingowe e-maile i wiadomości tekstowe mogą wskazywać, iż nadawcą jest instytucja współdziałająca ze strażą pożarną lub organ nadzorujący (Emergency Reporting, 2019).

Wszystkie analizowane incydenty naruszyły pośrednio zdolność operacyjną straży pożarnych, jednakże nie wpłynęły bezpośrednio na realizowanie ustawowych zadań. Nie oznacza to jednak, iż kolejne cyberataki nie wpłyną na zachowanie ciągłości operacyjnej straży pożarnej. Jak zauważa Greif, przed strażą pożarną stoi nowe wyzwanie, jakim jest cyberbezpieczeństwo. Nie jest to konieczność, którą można przypisać jedynie działom IT, ponieważ indeks możliwych podatności i narzędzi cyberbezpieczeństwa jest tak szeroki, że każdy z funkcjonariuszy musi posiadać przynajmniej podstawową wiedzę z przedmiotowego zakresu (Terrorism and Homeland Security Committee IAFCExternal, 2019, s. 2–16).

Analiza ryzyka w ataku ransomware

Jednym z największych zagrożeń dla cyberbezpieczeństwa w 2021 r. były ataki ransomware, czyli szkodliwe oprogramowanie wykorzystywane do szyfrowania danych w celu wymuszenia okupu za ich odzyskanie. CERT Polska zarejestrował 124 zdarzenia związane z tym zagrożeniem (jest to niespełna 13% więcej niż w roku 2020, w którym obsłużył 110 zdarzeń). Dla porównania, w 2019 r. CERT Polska obsłużył 26 incydentów związanych z infekcją ransomware (NASK, 2019, s. 9–16). W 2020 r. spośród 110 incydentów obsłużonych przez CERT Polska aż 69 zostało zgłoszonych m.in. przez krajowe instytucje publiczne (NASK, 2020, s.12–29). W 2021 r. administracja publiczna była celem takich ataków w 18 zdarzeniach (14,5% wszystkich incydentów ransomware) (NASK, 2021, s. 11–25).

Przeprowadzono analizę ryzyka ataku ransomware w obszarze działalności Państwowej Straży Pożarnej na gruncie lokalnych uwarunkowań.

Oszacowanie prawdopodobieństwa

- Przyjęto wartość P = 3 (umiarkowanie możliwe) ze względu na założoną częstotliwość wystąpienia co najmniej 1 raz na 5 lat w strukturze straży pożarnej.

Oszacowanie skutków

- poufność (Confidentiality) S = 4
- spójność/integralność (Integrity) S = 3
- dostępność (Availability) S = 4

Ryzyka operacyjne wynikające z zakłócenia kluczowych procedur PSP wspomaganych przez wymienione w pracy systemy:

- zablokowanie platformy bazodanowej na poziomie komend wojewódzkich oraz Komendy Głównej PSP (utrata ciągłości procesu)
- zablokowanie danych zawierających informacje o trwających czynnościach kontrolno-rozpoznawczych (utrata ciągłości procesu)

Analiza ryzyka w ataku phishing

W 2021 r. CERT Polska zarejestrował łącznie 29 483 unikalne incydenty cyberbezpieczeństwa, z czego najczęstszym typem ataku był phishing – stanowiący aż 76,57% wszystkich obsłużonych incydentów. Jest to wzrost o 196% w porównaniu do poprzedniego roku. W ostatnich latach ataki phishingowe stały się najczęstszą metodą kradzieży danych. Dla porównania w Stanach Zjednoczonych liczba takich ataków wzrosła o prawie 81,5% w ciągu zaledwie dwóch lat, a aż 74% organizacji amerykańskich doświadczyło udanego ataku phishingowego w 2020 r. (Blischoff, 2022). Liczba ataków phishingowych (Phishing/Vishing/Smishing/Pharming) w Stanach Zjednoczonych w latach 2019–2021 to zakres od 114 702 do 323 972 (Internet Crime Report, 2021, s. 3–30).

Według źródeł otwartych 15 marca 2020 r. miał miejsce atak phishigowy w straży pożarnej w Karolinie Południowej. Komputery zostały wyłączone przez hakera, a dane, pliki i wiadomości e-mail zostały zaszyfrowane.

Przeprowadzono analizę ryzyka ataku phishing w obszarze działalności Państwowej Straży Pożarnej na gruncie lokalnych uwarunkowań.

Oszacowanie prawdopodobieństwa

Przyjęto wartość P = 5 (prawie pewne) ze względu na założoną częstotliwość wystąpienia co najmniej 1 raz na miesiąc w strukturze straży pożarnej.

Oszacowanie skutków

- poufność (Confidentiality) S = 3
- spójność/integralność (Integrity) S = 2
- dostępność (Availability) S = 3

Ryzyka operacyjne wynikające z zakłócenia kluczowych procedur PSP wspomaganych przez wymienione w pracy systemy:
blokada służbowej poczty elektronicznej funkcjonariuszy i pracowników cywilnych PSP (utrata ciągłości procesu)

- wstrzymanie działania strony internetowej jednostki organizacyjnej PSP (utrata wizerunku).

Analiza ryzyka w ataku GPS spoofing

Spoofing danych GPS to próba oszukania odbiornika GPS poprzez emitowanie z powierzchni Ziemi fałszywego sygnału GPS. Wszystkie znajdujące się w pobliżu nawigacje zaczynają wyświetlać niepoprawną lokalizację. Atak ten może zostać wykorzystany do przechwycenia bezzałogowych statków powietrznych oraz wprowadzania w błąd operatorów dronów (Malenkovich, 2019).

Tego typu przypadki rejestruje Navigation Center United States Coast Guard U.S. Department of Homeland Security. Według danych otwartych opracowano jak dotąd trzy raporty zdarzeń dotyczących zakłócenia sygnału GPS podczas operowania dronami (GPS Problem Reports Status, 2022). Żadne z nich jak dotąd nie zakłóciło działań straży pożarnej, co może wynikać z faktu, iż technologia ta nie stanowi powszechnego elementu operacyjnego.

Przeprowadzono analizę ryzyka ataku GPS spoofing w obszarze działalności Państwowej Straży Pożarnej na gruncie lokalnych uwarunkowań.

Oszacowanie prawdopodobieństwa

Przyjęto wartość P = 2 (mało prawdopodobne) ze względu na założoną częstotliwość wystąpienia co najmniej 1 raz na 10 lat w strukturze straży pożarnej.

Oszacowanie skutków

	rutynowa interwencja	zdarzenie masowe
• poufność (Confidentiality)	S = 1	S = 2
• spójność/integralność (Integrity)	S = 1	S = 2
• dostępność (Availability)	S = 2	S = 3

Ryzyka operacyjne wynikające z zakłócenia kluczowych procedur PSP wspomaganych przez wymienione w pracy systemy:

- utrata urządzenia służącego do monitorowania rozwoju i rozprzestrzeniania się pożarów (nieprecyzyjne skierowanie sił i środków w przypadku pożaru lasu)
- utrata urządzenia służącego do monitorowania zagrożeń związanych z powodziami (utrudnienia operacyjne w działaniach ratowniczych oraz w ewakuacji poszkodowanych)
- utrata urządzenia służącego do prowadzenia działań poszukiwawczo-ratowniczych (nieodnalezienie osoby zaginionej w terenie otwartym, nieudzielenie pomocy)

Analiza ryzyka w ataku downlink intercept

Downlink intercept umożliwia dostęp do wszystkich danych przesyłanych między dronem a kontrolerem. Większość systemów komercyjnych dronów komunikuje się ze swoją bazą za pomocą niezaszyfrowanych kanałów komunikacyjnych, co w konsekwencji może stwarzać podatności w postaci przechwycenia i uzyskania dostępu do wrażliwych danych (Arampatzis, 2022). Przechwycenie danych pomiędzy dronem a bazą może być związane z ich

nieautoryzowanym wykorzystaniem, chyba że w oprogramowaniu zaimplementowano autodestrukcję danych, np. po wykryciu braku kontaktu jednostki BSP z bazą przez określony czas. Działania operacyjne, np. w akcjach poszukiwawczo-ratowniczych, coraz częściej charakteryzują się implementacją technologii BSP do sterowania którą najczęściej są wykorzystywane urządzenia mobilne oraz internet. Analiza danych otwartych wykazała, że powszechnie wykorzystywane drony charakteryzują się podatnością na cyberataki (Yaacoub, Noura, Salman, 2020).

Przeprowadzono analizę ryzyka ataku downlink intercept w obszarze działalności Państwowej Straży Pożarnej na gruncie lokalnych uwarunkowań.

Oszacowanie prawdopodobieństwa

Przyjęto wartość P = 1 (prawie niemożliwe) ze względu na założoną częstotliwość wystąpienia co najmniej 1 raz na 100 lat w strukturze straży pożarnej.

Oszacowanie skutków

	rutynowa interwencja	zdarzenie masowe
• poufność (Confidentiality)	S = 2	S = 3
• spójność/integralność (Integrity)	S = 1	S = 2
• dostępność (Availability)	S = 1	S = 2

Ryzyka operacyjne wynikające z zakłócenia kluczowych procedur PSP wspomaganych przez wymienione w pracy systemy:

- utrata materiału wideo zarejestrowanego w czasie katastrofy z udziałem wielu ofiar (niechroniony wizerunek osób poszkodowanych, który może dostać się do mediów)
- utrata materiału zdjęciowego pozyskanego w czasie katastrofy budowlanej (materiał miał być wykorzystany przez eksperta w celu określenia zagrożenia bezpieczeństwa konstrukcji i czynności stabilizujących)

Wystąpienie incydentu w rutynowym środowisku operacyjnym i w zdarzeniu masowym charakteryzuje się paradygmatem o istotnych zmiennych. W przypadku typowego działania operacyjnego incydent może wpłynąć na proces ratowniczy lub gaśniczy, lecz nie będzie znacząco obniżał zdolności

prowadzonych działań. Jednak w sytuacji zdarzenia masowego należy wziąć pod uwagę fakt, iż będzie się ono charakteryzowało dużą ilością poszkodowanych i ofiar, a incydent w tych warunkach może wielowymiarowo destabilizować działania operacyjne, co bezpośrednio może zagrażać bezpieczeństwu, w tym zdrowiu i życiu osób poszkodowanych. Ponadto jednostki organizacyjne ochrony przeciwpożarowej przetwarzają dane osobowe w związku z prowadzonymi działaniami ratowniczymi, w tym dane, które będą trafiać do systemu teleinformatycznego SWD PSP. Znajdują się w nim zarówno dane osobowe zwykłe, jak i dane osobowe wrażliwe (np. stan zdrowia poszkodowanego). Należy zatem założyć, iż utrata danych w zdarzeniu masowym będzie znacznie bardziej destabilizująca. Obliczone poziomy ryzyka poszczególnych zdarzeń zamieszczono w tabeli 1.

Tabela 1. *Wynik w ryzyka*

Zdarzenie	R (C)	R (I)	R (A)
Ransomware	**12**	9	**12**
Phishing	**15**	**10**	**15**
GPS Spoofing (drony)	2/4*	2/4*	4/6*
Przechwycenie danych (drony)	2/3*	1/2*	1/2*

*interwencja rutynowa/zdarzenie masowe

Źródło: opracowanie własne

Dyskusja

W przypadku wystąpienia incydentu w działaniach operacyjnych straży pożarnej w wyniku ataku ransomware istotnym potencjalnym skutkiem może być przerwanie procesów ciągłości działania. Ponadto dane operacyjne, w tym dane poufne, mogą zostać naruszone, co stanowi poważny problem w zakresie bezpieczeństwa danych. Wskazany w niniejszym opracowaniu przypadek ataku ransomware nie jest jedynym skierowanym na serwery służb mundurowych. Należy tu również wskazać na ataki w Roxana w stanie Illinois, Mount Pleasant, Karolina Południowa, a ostatnio w Atlancie w stanie Georgia. We wszystkich tego typu atakach zostały naruszone dane poufne (w tym dane osobowe).

W przypadku ataku phishing jako możliwe skutki w procesie operacyjnym można wskazać zakłócenia w przeciwdziałaniu skutkom awarii dla ludzi i środowiska, do których to zadań powołane są Państwowa (lub zakładowa) Straż Pożarna. Procesy takie jak ewakuacja ludności czy udzielanie kwalifikowanej pomocy medycznej mogą zostać opóźnione ze względu na paraliż systemów komputerowych będących w użytkowaniu służb ratowniczych.

Atak GPS spoofing może zakłócić odczyty nawigacji, która pozwala na obranie prawidłowego kierunku lotu drona. Spoofing GPS może wywołać zderzenie BSP z przeszkodą terenową lub jego przechwycenie i utratę zgromadzonych danych.

W przypadku ataku downlink intercept może dojść do przejęcia danych (w tym danych wrażliwych) przesyłanych między dronem a kontrolerem lotu.

We wszystkich wskazaniach w niniejszym opracowaniu potencjalnymi skutkami ataków cybernetycznych mogą być przerwane procesy w działaniach operacyjnych straży pożarnej, które w warunkach standardowego działania nie wpłyną znacząco na bezpieczeństwo zdrowia i życia poszkodowanych, to jednak w warunkach zdarzenia masowego mogą w istotnym stopniu zdestabilizować np. działania ratownicze. Ponadto wystąpienie poważnego incydentu w cyberprzestrzeni straży pożarnej może wpłynąć na utratę wizerunku organizacji bezpieczeństwa.

Wnioski

Celem niniejszego opracowania było dokonanie analizy dostępnych w źródłach otwartych incydentów w cyberprzestrzeni straży pożarnej oraz oszacowanie i zredukowanie ryzyka zaistnienia incydentów typu phishing i ransomware, a także powiązanych z wykorzystaniem bezzałogowych systemów powietrznych GPS spoofing oraz downlink intercept. Dotychczasowe cyberataki na straż pożarną zostały przeprowadzone głównie z wykorzystaniem techniki ransomware oraz phishing. Nie są to jedyne cyberzagrożenia, albowiem w dobie dynamicznie rozwijających się technologii wspierających działania operacyjne istotnym zagrożeniem są także ataki GPS spoofing oraz downlink intercept. Należy podkreślić, iż do cyberataków dochodziło

w standardowym środowisku operacyjnym. Jednak przy zmianie paradygmatu operacyjnego na zdarzenie masowe lub hybrydowe, materializowanie się zagrożeń cyberprzestrzeni może znacząco wpływać na zachowanie ciągłości operacyjnej. W związku z powyższym w niniejszym opracowaniu zaproponowano rekomendacje do strategii ograniczającej ryzyko operacyjne straży pożarnej w aspekcie cyberbezpieczeństwa oraz rekomendacje do polityki bezpieczeństwa z uwzględnieniem opracowanych ryzyk i działań korygujących (tabela 2). Powyższe rekomendacje powinny być uwarunkowane ciągłością oraz określoną metodologią wykorzystującą adekwatnie dobrany zestaw narzędzi. Rekomendacje ze względu na ograniczony zakres publikacji stanowią jedynie wektory wyznaczające główne kierunki w obszarze bezpieczeństwa w cyberprzestrzeni straży pożarnej.

Przyjmując, iż strategia to ogólny plan różnorakich działań, które powinny zakończyć się określonym rezultatem z określonym stanem rzeczy oraz prowadzeniem do określonego celu (w tym przypadku podniesienia odporności na cyberzagrożenia w systemach teleinformatycznych straży pożarnej), który jednocześnie powinien być wiodącym atrybutem w konstrukcji, rodzaju i charakterze strategii (Pazio, 2010) oraz na podstawie przeprowadzonych analiz w niniejszym opracowaniu zaproponowano pięć modułów strategii ograniczającej ryzyko operacyjne straży pożarnej w aspekcie cyberbezpieczeństwa:

1. Cel główny, cele szczegółowe oraz środki służące realizacji celów strategii;
2. Określenie środków w zakresie atrybutów bezpieczeństwa w cyberprzestrzeni: poufności, integralności, dostępności;
3. Działania prewencyjne;
4. Działania badawczo-rozwojowe w zakresie cyberbezpieczeństwa;
5. Zarządzanie strategią cyberbezpieczeństwa.

Cel strategii cyberbezpieczeństwa w straży pożarnej powinien być przede wszystkim kompatybilny z uwarunkowaniami prawnymi, Dyrektywą NIS 2 oraz Narodowymi Standardami Cyberbezpieczeństwa (NSC) a jego głównym atrybutem powinno być podniesienie odporności organizacji na zagrożenia systemów w cyberprzestrzeni operacyjnej i minimalizacja ryzyka, którego zmaterializowanie się może znacząco naruszyć realizację ustawowych

zadań organizacji. Cel główny może zostać osiągnięty poprzez realizację celów szczegółowych:

- Rozwój systemu cyberbezpieczeństwa w straży pożarnej poprzez: wdrożenie oraz ocenę funkcjonowania przepisów w zakresie cyberbezpieczeństwa, w tym także powołanie organu opiniodawczo-doradczego ds. cyberbezpieczeństwa oraz utworzenie formalno-organizacyjnego systemu wewnętrznego monitorowania środowiska cyberbezpieczeństwa w oparciu o analizę danych szczegółowych wszystkich jednostek organizacji; podniesienie poziomu efektywności systemu cyberbezpieczeństwa, w tym nadzór w zakresie systemów w straży pożarnej, działania wspierające operatorów i dostawców w zapewnieniu bezpieczeństwa świadczonych usług poprzez zalecenia organizacyjne i techniczne, udostępnione narzędzia oraz wiedzę w zakresie najlepszych praktyk podnoszących cyberbezpieczeństwo w straży pożarnej. Niezbędne jest także wdrożenie systemowego rozwiązania pozwalającego na wymianę informacji (wewnątrz i na zewnątrz) organizacji w zakresie podatności, zagrożeń i incydentów oraz rekomendacja modeli podnoszenia kwalifikacji w projektowaniu procesów zwiększających cyberbezpieczeństwo, a w szczególności w zakresie: doboru, wdrażania i utrzymania środków technicznych, w tym korzystania z nowoczesnych i bezpiecznych modeli przetwarzania w chmurach obliczeniowych, tworzenia bezpiecznych aplikacji oraz korzystania z bezpiecznych systemów mobilnych, a także wdrożenie standaryzacji rozwiązań zabezpieczających, w tym minimalnych wymagań bezpieczeństwa dla sieci i systemów teleinformatycznych w oparciu o NSC; rozbudowę systemu wymiany informacji na poziomie strategicznym i operacyjnym; wypracowanie i wdrożenie metodyki szacowania ryzyka w obszarze cyberbezpieczeństwa w oparciu o ramy zarządzania ryzykiem w organizacjach i systemach informatycznych; zwiększenie zdolności w zakresie zabezpieczenia dowodów przestępstw lub działalności o charakterze terrorystycznym.
- Podniesienie poziomu odporności systemów teleinformatycznych oraz osiągniecie zdolności do skutecznego zapobiegania i reagowania na incydenty poprzez opracowanie i wdrożenie standardów, dobrych

praktyk i zaleceń dla wszystkich jednostek organizacyjnych straży pożarnej oraz testy i audyty cyberbezpieczeństwa.
- Budowanie świadomości i kompetencji w zakresie cyberbezpieczeństwa w straży pożarnej poprzez zwiększenie kompetencji funkcjonariuszy i pracowników cywilnych; rozwijanie świadomości w kierunku bezpiecznego korzystania z cyberprzestrzeni.

Kolejny moduł strategii powinien definiować środki w zakresie atrybutów bezpieczeństwa w cyberprzestrzeni: poufności, integralności, dostępności. Do zabezpieczeń lub środków zaradczych stosowanych w systemie lub organizacji w celu ochrony poufności, integralności i dostępności systemu i jego informacji oraz zarządzania ryzykiem związanym z bezpieczeństwem informacji należą szeroko pojęte kontrole bezpieczeństwa. Kontrola prywatności natomiast to administracyjne, techniczne i fizyczne zabezpieczenia stosowane w systemie lub organizacji w celu zarządzania ryzykiem związanym z prywatnością i zapewnienia zgodności z obowiązującymi wymogami dotyczącymi prywatności. Kontrole bezpieczeństwa i prywatności są wybierane i wdrażane w celu spełnienia wymagań dotyczących bezpieczeństwa i prywatności nałożonych na system lub organizację. Wymogi dotyczące bezpieczeństwa i prywatności wynikają z obowiązujących przepisów, rozporządzeń wykonawczych, dyrektyw, przepisów, polityk, standardów i potrzeb związanych z misją w celu zapewnienia poufności, integralności i dostępności przetwarzanych, przechowywanych lub przesyłanych informacji oraz zarządzania zagrożeniami dla prywatności poszczególnych osób. Wybór i wdrożenie środków kontroli bezpieczeństwa i prywatności odzwierciedla cele programów bezpieczeństwa informacji i prywatności oraz sposób, w jaki programy te zarządzają związanym z nimi ryzykiem. W zależności od okoliczności cele i ryzyka mogą być niezależne lub nakładać się na siebie. Programy bezpieczeństwa informacji są odpowiedzialne za ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, użyciem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem (tj. nieupoważnioną działalnością lub zachowaniem systemu) w celu zapewnienia poufności, integralności i dostępności. Programy te są również związane z zarządzaniem ryzykiem bezpieczeństwa i zapewnieniem zgodności z obowiązującymi wymogami bezpieczeństwa. Programy ochrony

prywatności są odpowiedzialne za zarządzanie ryzykiem dla osób fizycznych związanym z tworzeniem, gromadzeniem, wykorzystywaniem, przetwarzaniem, przechowywaniem, konserwacją, rozpowszechnianiem, ujawnianiem lub usuwaniem (łącznie określanych jako „przetwarzanie") danych osobowych oraz za zapewnienie zgodności z obowiązującymi wymogami dotyczącymi prywatności (NIST Special Publication 800–853, 2020).

W zakresie modułu prewencyjnego strategii można wskazać kontrolę ryzyka wynikającego z podatności poprzez takie działania, jak:

- obrona – stosowanie zabezpieczeń, które eliminują lub zmniejszają pozostałe niekontrolowane ryzyko;
- przeniesienie – przeniesienie ryzyka do innych obszarów lub podmiotów zewnętrznych;
- łagodzenie – zmniejszanie wpływu zasobów informacyjnych w przypadku pomyślnego wykorzystania luki przez osobę atakującą;
- akceptacja – zrozumienie konsekwencji wyboru pozostawienia ryzyka bez kontroli, a następnie właściwe uznanie ryzyka, które pozostaje bez próby kontroli;
- eliminacja – usunięcie lub wycofanie zasobu informacyjnego ze środowiska operacyjnego organizacji (Whitman, Mattord, 2014).

W celu zapewnienia adekwatnej funkcjonalności, zarówno strategia jak i polityki bezpieczeństwa powinny odpowiadać rzeczywistym zagrożeniom. Stąd szczególnego znaczenia nabierają działania badawczo-rozwojowe, które powinny sprzyjać dogłębnemu zrozumieniu zagadnień związanych z systemami przeciwpożarowymi. Przykładem mogą tu być nowoczesne systemy zarządzania budynkiem zintegrowane z systemami ochrony przeciwpożarowej, które mogą stanowić istotną podatność w systemie. Jest to zagrożenie na tym etapie opracowane w nieznacznym zakresie. Zatem działania badawczo-rozwojowe w zakresie cyberbezpieczeństwa w straży pożarnej powinny uwzględniać ekspansywność podatności oraz dotkliwość konsekwencji a także świadomość społeczności straży pożarnej.

Zintegrowanym elementem strategii cyberbezpieczeństwa jest zarządzanie. Najczęściej przyjmuje się, iż jest to zarządzanie strategiczne będące definiowanym lub redefiniowanym procesem informacyjno-decyzyjnym

wspieranym przez takie funkcje, jak planowanie, organizacja, motywacja i kontrola (Sołtysik, 2016, s. 224–225). Zarządzanie strategiczne ma na celu zabezpieczenie organizacji w potencjale naruszenia lub zdestabilizowania ciągłości działania w oparciu o trzy etapy: analizę, planowanie oraz zarządzanie. Abstrahując od obszernych teorii zarządzania, w rozważanym przypadku warto nadmienić, iż proces ten powinien być oparty o fazy wynikające z ustawowych zadań straży pożarnej. Nie oznacza to, iż w ramach strategii nie można wykorzystać istniejących modeli zarządzania, lecz należy zwrócić uwagę, aby charakteryzowały one działania konkretnej organizacji.

Wskazany powyżej schemat strategii cyberbezpieczeństwa w straży pożarnej jest opracowaniem o charakterze dużej ogólności i jedynie wyznacza kierunki w środowisku dynamicznych zagrożeń dla systemów teleinformatycznych, lecz może stanowić wartość w procesie budowania cyberbezpieczeństwa w organizacji, którego istotnym elementem powinna być także polityka bezpieczeństwa. Politykę bezpieczeństwa można rozumieć jako podstawę do skutecznego i sprawnego funkcjonowania w organizacji poprzez podejmowanie zaplanowanych w niej działań ukierunkowanych na minimalizację strat w wyniku zagrożeń (Pazio, 2010). Celem polityki bezpieczeństwa w straży pożarnej powinno być podniesienie odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji operacyjnych. Elementami polityki bezpieczeństwa powinny być: dane poufne; ochrona urządzeń osobistych i służbowych; bezpieczeństwo środków komunikacji elektronicznej; zarządzanie hasłami i kodami dostępu; bezpieczne przesyłanie danych i informacji operacyjnych. Ponadto w celu zminimalizowania ryzyk związanych z naruszeniem bezpieczeństwa, należy wprowadzić dodatkowe środki wynikające z cyberhigieny. W tym celu można wykorzystać zawarte w tabeli 2 wskazania redukujące ryzyko w zakresie podstawowej wiedzy zabezpieczającej systemy teleinformatyczne w straży pożarnej (tabela 2).

W aspekcie podjętego celu oraz problemu badawczego można jednoznacznie stwierdzić, iż incydenty w cyberprzestrzeni straży pożarnej mogą wpływać na funkcjonowanie bazodanowych systemów wspomagania decyzji, a tym samym mogą realnie naruszyć lub przerwać ciągłość działań operacyjnych straży pożarnej. W przypadku działania w środowisku standardowego zdarzenia incydent nie zdestabilizuje czynności operacyjnych, jednak w sytuacji

zdarzenia masowego naruszenie bezpieczeństwa systemów teleinformatycznych może w dużym stopniu wpływać na jakość i czas wykonywanych działań ratowniczo-gaśniczych.

Tabela 2. *Wartości ryzyka ze wskazaniem działań korygujących*

Lp.	Obszar i wartość ryzyka	Strategie postępowania
1.	Phishing R (C) = 15 R (I) = 10 R (A) = 15	1. Zdobywać bieżącą wiedzę na temat najnowszych technik phishingowych 2. Nie otwierać linków przesłanych w przypadkowych i podejrzanych e-mailach 3. Zainstalować w przeglądarce pasek narzędzi antyphishingowych 4. Weryfikować bezpieczeństwo witryny (sprawdzić: adres URL witryny zaczynający się od https, ikonę zamkniętej kłódki w pobliżu paska adresu, certyfikat bezpieczeństwa witryny) 5. Regularnie zmieniać hasła we wszystkich kontach internetowych 6. Aktualizować przeglądarkę internetową 7. Korzystać z zapór sieciowych 8. Nigdy nie wysyłać danych osobowych (jedynie w postaci zaszyfrowanej i tylko do zaufanych odbiorców)
2.	Ransomware R (C) = 12 R (A) = 12	1. Wdrożyć proaktywność (plan ciągłości działania musi być praktycznie testowany poprzez symulacje zdarzeń prowadzonych według realistycznych scenariuszy) 2. Edukować pracowników w zakresie cyberbezpieczeństwa i świadomości zagrożeń phishingu 3. Zastosować proces uwierzytelniania wieloskładnikowy lub dwuetapowy 4. Przeprowadzać update-y i aktualizacje systemów 5. Zainstalować i odpowiednio skonfigurować narzędzia do wykrywania i reagowania na te zdarzenia 6. Zaprojektować sieci, systemy i tworzenie kopii zapasowych, aby zmniejszyć wpływ podatności oprogramowania na atak ransomware 7. Rozważyć opcję przeniesienia ryzyka (np. na dostawców usług) 8. Utworzyć zewnętrzny zespół reagowania kryzysowego
3.	GPS Spoofing (drony) dla zdarzenia masowego R (A) = 6	1. Ograniczyć obecność postronnych osób na miejscu akcji 2. Zainstalować dodatkową antenę służącą do weryfikacji sygnału, mającą pomóc w określeniu, która antena jest celem ataku 3. Przełączyć włączone urządzenia GPS w tryb offline, gdy nie są używane (np. podczas lotu w zasięgu wzroku VLOS)

Źródło: opracowanie własne na podstawie (2021 Global Risk Managment Survey, 2021, s. 1-53; Yasar, 2021).

References

Arampatzis, A. (2022). *Bezpieczeństwo cybernetyczne a drony: Jak radzić sobie z zagrożeniami dla bezpieczeństwa*,https://sklep.pf-electronic.pl/pl/blog/Bezpieczenstwo-cybernetyczne-a-drony-Jak-radzic-sobie-z-zagrozeniami-dla-bezpieczenstwa/2144, (dostęp: 27.10.2022).

Bischoff, P. (2022). *Ransomware attacks on US government organizations cost over $70bn from 2018 to October 2022*,https://www.comparitech.com/blog/information-security/government-ransomware-attacks/, (dostęp: 23.10.2022).

Blischoff, P. (2021). *The State of Phishing in the US: Report and Statistics 2021*,https://www.comparitech.com/blog/information-security/state-of-phishing/, (dostęp: 23.10.2022).

Brooks, Ch.J., Grow, Ch., Craig, P. Short D. (2018). *Cybersecurity Essentials*, Sybex.

Chevreaux, J. Owen, P. Donaldson, K. Bright, K. Largen, A. Meiselman, D. Kirsanova, K. Borinski, M. Uribe, A. (2021). *Cybersecurity for Fire Protection Systems. Final Report. Fire Protection Research Foundation, Quincy (MA, USA).*

Chevreaux, J., Owen, P., Donaldson, K., Bright, K., Largen, A., Meiselman, D., Kirsanova, K., Borinski, M., Uribe, A. (2021). *Cybersecurity for Fire Protection Systems*. NFPA, https://www.nfpa.org/-/media/Files/News-and-Research/Fire-statistics-and-reports/Building-and-life-safety/RFCybersecurity.pdf, (dostęp: 23.10.2022).

Cooper, H. *Government agencies are conducting more and more services online, but they are struggling to stay ahead of hackers trying to steal valuable personal information*. w: *Protecting against cyberattacks: a guide for public safety leaders*, https://www.iafc.org/docs/default-source/1comm-tech/protecting-against-cyberattacks-magazine_final.pdf?sfvrsn=584e810d_0, (dostęp: 14.10.2022).

Dupuy, A., Nussbaum, D., Butrimas, V., Granitsas, A., *Bezpieczeństwo energetyczne w czasach wojny hybrydowej,* https://www.nato.int/docu/review/pl/articles/2021/01/13/bezpieczenstwo-energetyczne-w-czasach-wojny-hybrydowej/index.html, (dostęp: 14.10.2022).

Emergency Reporting. (2019). https://www.firehouse.com/tech-comm/computers-accessories/blog/21112107/emergency-reporting-industry-insights-cyber-attack-security-basics-hacking-protection-firefighters, (dostęp:19.10.2022).

ENISA. (2021). *Raport Enisa Threat Landscape*.

Federal Bureau of Investigation, Internet Crime Report. (2021). https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, (dostęp: 16.10.2022).

Feltynowski, M. (red.). (2019). *Wykorzystanie bezzałogowych platform powietrznych w operacjach na rzecz bezpieczeństwa publicznego*. Józefów: Wyd. CNBOP-PIB.

Garbe, W. (2018). *Ransomware Attacks Against Riverside, Ohio, Worse than Initially Thought*, https://www.govtech.com/security/ransomware-attacks-against-riverside-ohio-worse-than-initially-thought.html, (dostęp: 16.10.2022).

Global Risk Management Survey. (2021). AON, Cover – 2021 Global Risk Management Survey (aon.com), (dostęp: 29.10.2022).

Kosik, J. *What Fire Departments Can Do to Combat Ransomware*, https://www.firehouse.com/tech-comm/news/12374041/what-firefighters-fire-departments-can-do-to-combat-hacking-malware-ransomware-firefighter-news, (dostęp: 16.10.2022).

Liwo, M.A. (2020). Państwowa Straż Pożarna jako jeden z zasadniczych podmiotów publicznych w sprawach zapewnienia określonego rodzaju bezpieczeństwa i porządku. *Przegląd Prawa Publicznego*, (11), 105–132.

Maia, E., Praça, I., Mantzana, V., Gkotsis, I., Petrucci, P., Biasin, E., Kamenjasevic, E., Lammari, N. W: Soldatos, J., Philpot, J., Giunta, G. (red.). (2020). *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures, Boston-Delft*, http://dx.doi.org/10.1561/9781680836875, (dostęp: 10.10.2022); zob. także: *Cyberbezpieczeństwo w ochronie zdrowia 2022 – raport.*

Malenkovich, S. (2019). Czy można zabezpieczyć się przed fałszowaniem sygnału GPS. *Kaspersky Daily*, https://plblog.kaspersky.com/gps-spoofing-protection/10745/, (dostęp: 24.10.2022).

NASK. *Raport roczny*. (2019). https://cert.pl/uploads/docs/Raport_CP_2019.pdf, (dostęp: 22.10.2022).

NASK. *Raport roczny*. (2020). https://cert.pl/uploads/docs/Raport_CP_2020.pdf, (dostęp: 22.10.2022).

NASK. *Raport roczny*. (2021), https://cert.pl/uploads/docs/Raport_CP_2021.pdf, (dostęp: 23.10.2022).

Navigation Center United States Coast Guard U.S. Department of Homeland Security. (2022).*GPS Problem Report Status*, https://www.navcen.uscg.gov/gps-problem-report-status, (dostęp: 27.10.2022).

Nowakowski, M. (2019). Nowe wytyczne EBA w sprawie zarządzania ryzykami IT oraz bezpieczeństwa. Cz. 1. Definicja, strategia i strony trzecie. *Bankowość PSD2*, https://finregtech.pl/2019/12/02/jest-troche-zmian-a-czasu-malo-nowe-wytyczne-eba-w-sprawie-zarzadzania-ryzykami-it-oraz-bezpieczenstwa-cz-1-definicja-strategia-i-strony-trzecie/.

Rector, K. *Baltimore Officials: 911 System Was Hacked*, https://www.firehouse.com/tech-comm/cad-dispatch-systems/news/20998605/baltimore-md-911-system-hacked-firefighters-, (dostęp: 17.10.2022).

Rządowe Centrum Bezpieczeństwa. (2021). Narodowy Program Ochrony Infrastruktury Krytycznej (Załącznik 1), Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje. Warszawa.

Terrorism and Homeland Security Committee IAFC External. *Protecting against cyberattacks: a guide for public safety leaders,* https://www.iafc.org/docs/default-source/1comm-tech/protecting-against-cyberattacks-magazine_final.pdf?sfvrsn=584e810d_0, (dostęp: 19.10.2022).

The Island Packet. *Hacker Holds SC Fire Department Hostage amid Pandemic,* https://www.firehouse.com/tech-comm/news/21130618/hacker-holds-sc-fire-department-hostage-amid-pandemic, (dostęp: 17.10.2022).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz. U. 2002 Nr. 144 poz. 1204.

Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej art. 1. Dz. U. 1991 Nr 88 poz. 400.

Yaacoub, J.P., Noura, H., Salman, O., Chehab, A. (2020). *Security analysis of drones systems: Attacks, limitations, and recommendations, Internet of Things*, Vol. 11.https://www.sciencedirect.com/science/article/pii/S2542660519302112, (dostęp: 27.10.2022).

Yasar, Kinza. (2021). *What is GPS Spoofing? How to Guard Against GPS Attacks*, https://www.makeuseof.com/what-is-gps-spoofing-how-to-guard-against-gps-attacks-/, (dostęp: 29.10.2022).

Whitman, M. E., &Mattord, H. J. (2014). *Management of information security* (4th ed.). Stanford, CT: Cengage Learning.

Zegarow, P. (2019). Dlaczego wierzymy w dezinformację, analiza mechanizmów psychologicznych. W: NASK, *Zjawisko dezinformacji w dobie rewolucji cyfrowej*,https://cyberpolicy.nask.pl/1577-2/, (dostęp: 23.10.2022).

Zwęgliński, T., Smolarkiewicz, M., Gromek, P. (2020). *Efekt kaskadowy współczesnym wyzwaniem zarządzania kryzysowego*. Warszawa: SGSP.