ISSN 2300-5149

PRZEGLĄD TELEINFORMATYCZNY

TOM 10 (28) **Nr 1-4 (52)**
WARSZAWA **2022**

PRZEGLĄD TELEINFORMATYCZNY
TELEINFORMATICS REVIEW

Dawniej: BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI WAT
(ISSN 1427-3578) https://bibliotekanauki.pl/journals/289/issues
Ukazuje się od 1995 r.

ADRES REDAKCJI
Redakcja Przeglądu Teleinformatycznego
00-908 Warszawa, ul. gen. Sylwestra Kaliskiego 2
tel. 261 83 87 03, fax. 261 83 71 44
e-mail: pt [at] ita.wat.edu.pl

WWW: **https://przegladteleinformatyczny.publisherspanel.com/**
http://przeglad.ita.wat.edu.pl/

Wersją pierwotną czasopisma jest wersja elektroniczna

REDAKTOR NACZELNY:
Antoni Donigiewicz

REDAKTOR WYDANIA
Antoni Donigiewicz

OPRACOWANIE STYLISTYCZNE
Renata Borkowska

PROJEKT OKŁADKI
Barbara Chruszczyk

WYDAWCA: Instytut Teleinformatyki i Cyberbezpieczeństwa WAT

ISSN 2300-5149
ISSN 2353-9836 (on-line)

Narzędzie do wspomagania migracji systemów informacyjnych organizacji do „Zero Trust Architecture”

Weronika BURAS

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
weronika.buras77@gmail.com

STRESZCZENIE: W artykule przedstawiono podstawowe informacje na temat koncepcji „Zero Trust Architecture” oraz projekt i wykonane na jego podstawie narzędzie do wspomagania migracji systemów informacyjnych do „Zero Trust Architecture”. We wstępnej części artykułu opisano zwięźle koncepcję Zero Trust oraz przedstawiono wykonaną na bazie NSC 800-207 listę czynności niezbędnych do migracji systemów informacyjnych do wyżej wymienionej architektury. Następnie zaprezentowano procedurę praktycznego wykorzystania tej listy. Na końcu artykułu krótko opisano sposób implementacji wspomnianej procedury do postaci narzędzia wspomagającego migrację.

SŁOWA KLUCZOWE: system informacyjny, architektura Zero Trust, architektura zerowego zaufania, bezpieczeństwo systemów informacyjnych, NSC 800-207, NIST SP 800-207

1. Wstęp

W obecnych czasach dynamicznego rozwoju technologii nieodłączną częścią życia stały się systemy informacyjne, które pomagają usprawnić oraz udoskonalić działania organizacji, nie czynią jej jednak bardziej nowoczesną [3]. Wraz z rozwojem technologicznym wzrosło ryzyko niepożądanych działań na przechowywanych w systemach informacyjnych danych. Coraz większą wagę zaczęto zatem przypisywać bezpieczeństwu systemów informacyjnych, w tym ochronie danych, które to dane nierzadko są składowymi informacji wrażliwych. W przypadku bardziej rozbudowanych systemów zaczynają pojawiać się pytania: „kto powinien mieć dostęp do danej bazy danych?” „kto powinien posiadać jakie

uprawnienia?". Łatwo mylnie połączyć nitki w sieci relacji, jakie budują się w takiej sytuacji. Należy przede wszystkim wziąć pod uwagę minimalne uprawnienia do działania w systemie informacyjnym dla konkretnego użytkownika, bez których nie zostanie zapewniona skuteczna ochrona danych przed nieuprawnionym dostępem w takim systemie przetwarzanych.

Z pomocą przychodzą zalecenia opracowane chociażby przez takie organizacje, jak National Institute of Standards and Technology – w skrócie NIST[1]. Koncepcja Zero Trust (dalej w skrócie ZT) Architecture została przedstawiona już w 2010 roku przez głównego analityka firmy Forrester Johna Kindervag [12]. Jej podstawą jest traktowanie każdego użytkownika jako niezaufanego przy każdym wymaganym przez niego dostępie do zasobu informacyjnego, nawet gdy wcześniej w tym systemie poprawnie się uwierzytelnił.

Na The H@ck Summit [13] organizowanym w 2021 oraz 2022 roku architektura zerowego zaufania stałą się głównym tematem kilku wideokonferencji. Sama idea ZT była znana wcześniej, jednak dopiero teraz została sformalizowana.

2. Koncepcja „Zero Trust Architecture"

Koncepcja architektury zerowego zaufania opiera się na zasadzie „Nigdy nie ufaj, zawsze weryfikuj". Jest to strategiczne podejście do zagadnienia cyberbezpieczeństwa. Założeniem jest zabezpieczenie organizacji poprzez ciągłą weryfikację uprawnień dostępu oraz eliminację „ślepego zaufania" użytkownikowi bądź zasobowi. ZT powstało w oparciu o spostrzeżenie, że według „klasycznych" paradygmatów udzielania dostępu użytkownikom, wszystko w sieci przedsiębiorstwa powinno być domyślnie zaufane. Oznacza to, że po uwierzytelnieniu się w sieci użytkownik zarówno w roli pracownika, klienta, jak i cyberprzestępcy, może uzyskiwać dostęp do różnych jej zasobów bez dodatkowych sprawdzeń tożsamości. Zaimplementowanie koncepcji ZT ogranicza zaufanie oraz dostęp do zasobów do minimum. Każdy użytkownik czy urządzenie, nawet to, które znajduje się wewnątrz systemu, jest traktowane jako potencjalnie niebezpiecznie i podlega uwierzytelnieniu.

Według artykułu [11] opublikowanego przez firmę Spanning, co 39 sekund strona internetowa jest atakowana. Biorąc pod uwagę możliwe sposoby ataku, takie jak np. eskalacja uprawnień czy wykorzystanie typowych danych do

[1] NIST (ang. National Institute of Standards and Technology) jest amerykańską agencją federalną zajmującą się dostarczaniem standardów w zakresie bezpieczeństwa IT. Opracowane przez nią normy są dostępne dla wszystkich użytkowników bezpłatnie. Korzystają z nich przede wszystkim organizacje rządowe.

uwierzytelniania, istotnym zadaniem dla osób odpowiedzialnych za bezpieczeństwo systemów informacyjnych organizacji jest ograniczenie takich możliwości.

Zastosowanie Zero Trust Architecture w systemie informacyjnym jest koncepcją, która jest w opozycji dla dotąd rozpowszechnianej koncepcji „pojedynczego punktu uwierzytelniania” (ang. Single Sign On – SSO). Warto zauważyć, że jej założenia nie skupiają się na poprawie zaimplementowanego kodu, obsłudze błędów czy blokowaniu możliwych luk w systemie – istotą jest kontrola dostępu do danych oraz zasobów. Jak podaje firma Microsoft, która również dołączyła do swojej oferty [20] migrację zgodną z modelem Zero Trust, w tej architekturze weryfikuje się każde żądanie do dowolnego zasobu, jakby pochodziło z sieci zewnętrznej – nie istnieje pojęcie zaufanej sieci bądź zasobu. Przed udzieleniem dostępu niezbędne jest uwierzytelnienie oraz sprawdzenie autoryzacji użytkownika. Mikrosegmentacja sieci oraz zasada przydzielania najniższych uprawnień wspomaga główną ideę ZT.

Według zleconego przez firmę Microsoft badania Total Economic Impact [10], które przeprowadziła firma Forrester Consulting, zwrot z inwestycji, jakim jest zastosowanie rozwiązania Zero Trust, wskazuje na oszczędności i korzyści biznesowe na poziomie 92%.

Według artykułu [22] opublikowanego przez Palo Alto Networks architektura ZT ma na celu ochronę środowiska informatycznego, z którego korzysta organizacja poprzez segmentację sieci, silne metody uwierzytelniania, uproszczenie zasad przyznawania możliwie najniższego dostępu oraz poprzez ochronę przed zagrożeniami w warstwie 7 modelu OSI/ISO.

Według Rajiv Raghunarayana [19] wdrożenie koncepcji architektury ZT:

- Zmniejsza możliwości ataku na zasoby informacyjne organizacji.
- Wymusza w organizacji proaktywne działania w zakresie bezpieczeństwa informacyjnego.

Największe znaczenie dla praktycznego zastosowania koncepcji ZT, zdaniem autorki tego artykułu, miał standard *Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”* [17] o symbolu NSC 800-207, który z tego powodu zostanie nieco dokładniej przedstawiony w kolejnym rozdziale.

3. Przegląd publikacji NSC 800-207

Standard *Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”* [17] o symbolu NSC 800-207 jest polską wersją

dokumentu Zero Trust Architecture [9] o symbolu NIST SP (Special Publication) 800-207. Tłumaczeniem zajął się Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów. 7 września 2021 r. przetłumaczona publikacja została opublikowana z symbolem NSC 800-207.

Publikacja NIST SP 800-207 została oficjalnie przekazana do użytku publicznego dnia 11 sierpnia 2021 r. Zanim to nastąpiło, wydane zostały dwa szkice – 23 września 2019 r. oraz 13 lutego 2020 r. Każda z wersji publikacji jest dostępna na stronie NIST [6].

Publikacja NSK 800-207 została opublikowana dnia 7 września 2021 r. przez Serwis Rzeczypospolitej Polskiej. Jest ona ogólnie dostępna i skierowana głównie do pracowników zajmujących się bezpieczeństwem systemów teleinformatycznych. Składa się z siedmiu rozdziałów:

- rozdział 1 zawiera informacje o strukturze dokumentu oraz próbach wdrożenia zasad ZT w amerykańskich instytucjach federalnych;
- rozdział 2 składa się z definicji i założeń dotyczących architektury ZT;
- rozdział 3 zawiera definicje bloków konstrukcyjnych, które leżą u podstawy architektury ZT oraz komponentów logicznych;
- rozdział 4 jest opisem możliwych przypadków użycia architektury ZT, w których jej zastosowanie powoduje zwiększenie bezpieczeństwa przetwarzania danych oraz pozwala je uczynić mniej podatnymi na ataki;
- rozdział 5 zawiera opis sposobów realizacji zagrożeń, które mogą dotyczyć przedsiębiorstwa organizacji korzystających z architektury ZT;
- rozdział 6 jest porównaniem założeń ZT z już istniejącymi wytycznymi dla przedsiębiorstw publicznych;
- rozdział 7 zawiera opis czynności, które należy wykonać w trakcie planowania oraz wdrażania infrastruktury opartej na architekturze ZT.

Kluczowymi rozdziałami, których zawartość została wykorzystana w procesie opracowywania opisanej dalej procedury i jej implementacji, są rozdziały 2 oraz 7. Zdefiniowana jest w nich architektura ZT oraz niezbędne czynności jakie należy wykonać przy próbie migracji do niej. Zawarte w nich informacje były podstawą do zbudowania skomputeryzowanej procedury migracji do architektury ZT według zaleceń NSC 800-207. Posłużyły także do wykonania listy sprawdzeń kompletności spełnienia zaleceń NSC, która może zostać wykorzystana w trakcie audytu (weryfikacji) procesu migracji (patrz rozdz. 4.1).

4. Procedura wspomagająca implementację zaleceń NSC 800-207

W rozdziale drugim *Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania”* opisano podstawy architektury ZT, a w siódmym – proces migracji. Na ich podstawie opracowano procedurę, która wspomaga migrację systemu informatycznego do architektury Zero Trust. Zawiera ona zarówno wytyczne, co należy zrobić w celu uzyskania zgodności systemu z zaleceniami NSC 800-207, jak i czynności w przypadku niespełnienia jakiejś wytycznej. Procedura skierowana jest do pracowników działu bezpieczeństwa, administratorów oraz innych pracowników przedsiębiorstwa, których zadaniem jest migracja zarządzanego systemu informatycznego do ZTA.

4.1. Procedura migracji systemu informatycznego do architektury zerowego zaufania

Rysunek numer 1 przedstawia fragment procedury migracji do architektury Zero Trust. Procedura składa się z listy 21 czynności, które należy wykonać w celu migracji. Każdy punkt listy zawiera specyfikację działań, jakie trzeba wykonać, aby dane zalecenie NSC 800-207 zostało spełnione, a także komentarze i uwagi wykonawcze. Specyfikacja działań zawiera między innymi przykładową interpretację analizy ryzyka zamieszczona w pracy [2]. Procedura może zostać również wydrukowana i uzupełniona analogicznie do jej skomputeryzowanej wersji. Na końcu procedury w postaci „papierowej” znajduje się miejsce na komentarz do całej procedury, w których wypełniający procedurę może zapisać uwagi bądź spostrzeżenia.

Sporządzona została również lista pytań kontrolnych, której fragment został przedstawiony na rysunku numer 2. Zawiera ona tak zwane checkbox, które służą do zaznaczenia odpowiedniej odpowiedzi np. podczas przeprowadzanego audytu poprawności i kompletności wdrożenia zaleceń migracyjnych. Lista ta może zostać wykorzystana w celu dalszego rozwoju opisanego w tym artykule oprogramowania o dodatnie funkcjonalności sprawdzenia zgodności z zaleceniami standardu.

PROCEDURA MIGRACJI DO ARCHITEKTURY ZERO TRUST

(na podstawie NSC 800-207)

1. **Sprawdź, czy jest zatwierdzona lista zasobów w sieci przedsiębiorstwa. Jeśli tak wykonaj czynność z punktu 2, w przeciwnym wypadku wykonaj czynność z punktu 1.1**

   1.1.

   a. Przeanalizuj źródła danych dostępnych w przedsiębiorstwie oraz usługi.

   b. Wyznacz te z nich, które będą uznawana za zasoby.

   c. Zapisz wyznaczone zasoby w dokumencie polityki.

d. Udostępnij dokument zgodnie z polityką bezpieczeństwa w przedsiębiorstwie.

UWAGA! W pozostałych pytaniach używane określenie zasoby będzie odnosiło się do listy zasobów określonych w pytaniu numer 1. Zatem aby móc spełnić dane wymaganie konieczne jest spełnienie warunku 1.

2. **Jeżeli dostęp do zasobów przyznawany jest zawsze na zasadzie SSO (Single Sign On) to wykonaj czynności z punktu 3, w przeciwnym przypadku wykonaj czynności z punktu 2.1.**

   2.1.

   a. Wyznacz zasady uwierzytelniania oraz autoryzacji użytkownika.

   b. Zapisz wyznaczone zasady w dokumencie polityki.

   c. Wprowadź zmiany określone w dokumencie polityki.

Komentarz:

Proces uwierzytelniania i autoryzacji powinien być przeprowadzony bezwzględnie przed każdorazowym dostępem do zasobu.

Rys. 1. Fragment procedury migracji do architektury Zero Trust

1. **Czy istnieje zatwierdzona lista zasobów w sieci przedsiębiorstwa?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐ POTRZEBNY KOMENTARZ

2. **Czy w przedsiębiorstwie <u>każdorazowy dostęp</u> do zasobów przyznawany jest na zasadzie SSO (Single Sign On – po <u>jednorazowym</u> uwierzytelnieniu uzyskiwany jest dostęp do wszystkich zasobów)?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐ POTRZEBNY KOMENTARZ

3. **Czy <u>cała</u> komunikacja w sieci pomiędzy podmiotami w przedsiębiorstwie jest zabezpieczona bez względu na ich lokalizację?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐ POTRZEBNY KOMENTARZ

4. **Czy dostęp do poszczególnych zasobów przedsiębiorstwa przyznawany jest z <u>najniższymi możliwymi</u> wymaganiami?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐POTRZEBNY KOMENTARZ

5. **Czy polityka, o której mowa w punkcie 6 określa również inne behawioralne oraz środowiskowe cechy?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐ POTRZEBNY KOMENTARZ

6. **Czy w przedsiębiorstwie istnieją są stosowane mechanizmy integralności?**

   ☐ TAK ☐ NIE ☐ NIE DOTYCZY ☐ POTRZEBNY KOMENTARZ

Rys. 2. Lista sprawdzeń zgodności z założeniami zaleceń NSC 800-207

4.2. Instrukcja użycia oprogramowania wspomagającego migrację systemu informatycznego do architektury zerowego zaufania

Po pomyślnym uwierzytelnieniu oraz autoryzacji użytkownik ZTA Migration App (tak nazwano oprogramowanie wspomagające migrację) może przystąpić do procesu migracji, wykorzystując w tym celu skomputeryzowaną wersję procedury i wybierając panel aplikacji o nazwie *Nowa Procedura*. Zalecane jest wykonywanie procedury w kolejności wypisanych czynności. Należy z niej korzystać w następujący sposób:

POCZĄTEK

1. Po przystąpieniu do wykonywania listy czynności uzupełnij nazwę systemu.
2. Przejdź do pierwszego opisu czynności.

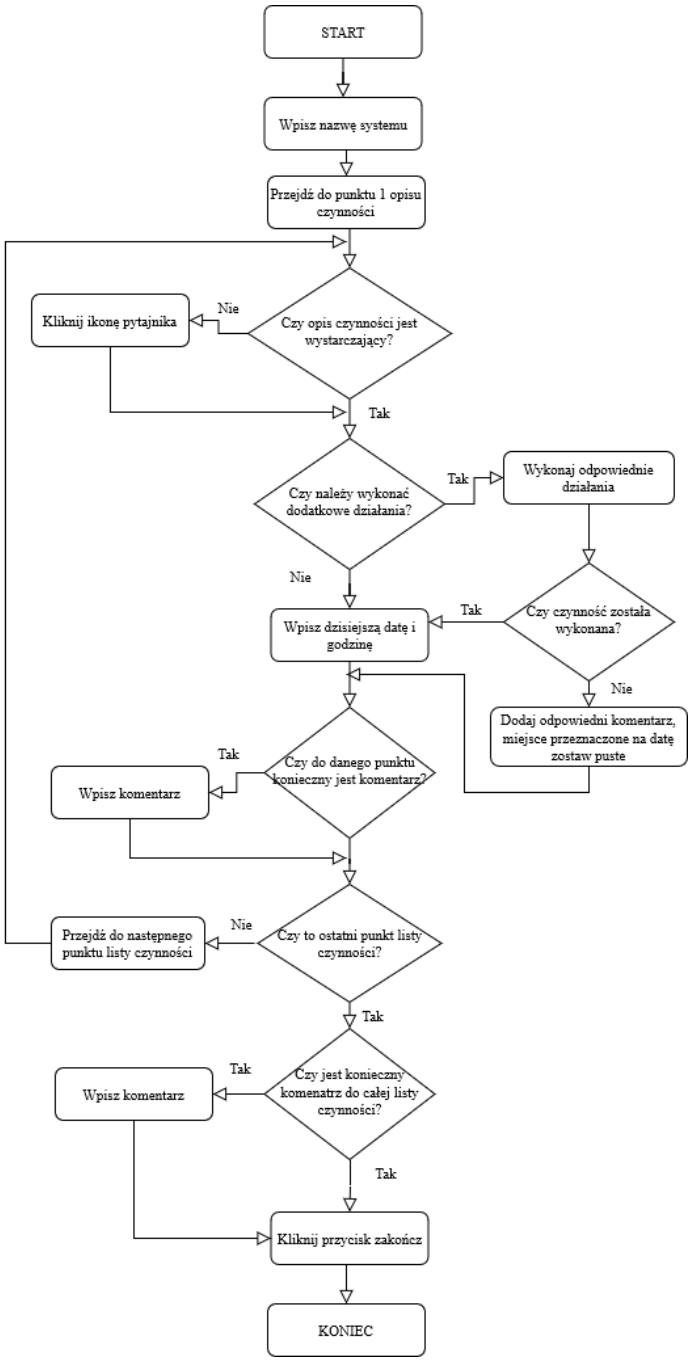
2.1. Jeżeli nie jest konieczne podjęcie żadnych działań (patrz ostatnie zdanie opisu czynności), należy wpisać dzisiejszą datę.
2.2. Jeśli opis czynności jest niewystarczający, kliknij w ikonę pytajnika po prawej stronie. Zostanie otwarte okno z szerszym opisem.
2.3. Jeśli konieczne jest wykonanie dodatkowych czynności – podejmij je, a następnie wpisz datę zakończenia.
2.3.1. Jeśli jakaś czynność nie została wykonana, należy zostawić puste miejsce przeznaczone na datę oraz dodać komentarz.
2.4. Jeśli jest konieczny, zapisz komentarz w polu tekstowym obok.
3. Przejdź do następnego opisu czynności i postępuj analogicznie do punktu 2.
4. Po zakończeniu ostatniego punktu z listy, jeśli istnieje taka konieczność, należy wpisać komentarz. Następnie kliknij przycisk zakończ.

KONIEC

Zapis tej instrukcji w pseudokodzie ma postać:

```
/* Instrukcja użycia narzędzia ZTA Migration App */
BEGIN
    Input systemName:
    For each numberOfActivities
            IF  noActivityIsNeeded
                Input endDate
            ELSE
                Perform necessary actions
                Input endDate
            END IF
            IF helpIsNeeded
                Click questionMarkButton
            END IF
            IF commentIsNeeded
                Input comment
            END IF
    END FOR
            IF commentToAllIsNeeded
                Input commet
            END IF
    Click endProcedureButton;
END
```

Na rysunku 3 instrukcja ta jest przedstawiona w postaci schematu blokowego.

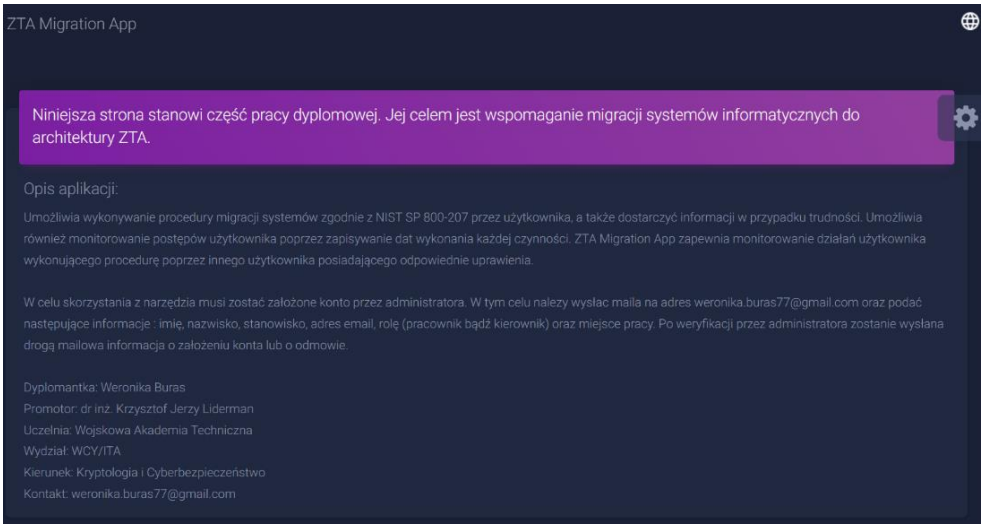


Rys. 3. Diagram sekwencji przedstawiający sposób użycia listy czynności

Po zakończeniu wykonywania instancji roboczej procedury możliwe jest wypisanie potrzebnych komentarzy i uwag przez osobę wypełniającą. W przypadku wersji elektronicznej, po kliknięciu odpowiedniego przycisku zostanie wygenerowany raport, którego fragment jest widoczny na rysunku numer 5, zawierający wykonywaną procedurę, dane użytkownika, który ją wykonywał oraz dane systemu informatycznego, jakiego ona dotyczyła. Możliwe jest wygenerowanie do wskazanego pliku (umożliwienie wydrukowania) informacji o zakończonej procedurze, dacie oraz o osobie, która zajmowała się tym procesem.

5. Oprogramowanie wspomagające proces migracji systemu informatycznego do architektury zerowego zaufania

W ramach pracy [1] zostało opracowane oprogramowanie (narzędzie) o nazwie ZTA Migration App wspomagające proces migracji systemu informatycznego do architektury zerowego zaufania zgodnie z zaleceniami NSC 800-207 (patrz rys. 4). Aplikacja jest udostępniona w Internecie z wykorzystaniem narzędzia Azure. Fragment strony startowej jest przedstawiony na rysunku 4.



Rys. 4. Strona startowa ZTA Migration App

Przyjęto założenia, że oprogramowanie ZTA Migration App ma:

- wspomóc wykonywanie procedury migracji;
- dostarczyć informacji, w razie potrzeby, nt. realizowanych czynności;
- umożliwić monitorowanie postępów migracji poprzez zapisywanie dat wykonania każdej czynności;
- dostarczyć wykresu postępów migracji (patrz rys. 5);
- zapewnić możliwość kontroli postępów migracji przez posiadającego odpowiednie uprawienia nadzorcę;
- umożliwić archiwizację raportów z przebiegu procesu migracji w odpowiednio zabezpieczonej bazie danych.

Projekt narzędzia w architekturze klient-serwer wykonano metodą obiektową.

Do projektowania oprogramowania wykorzystano:

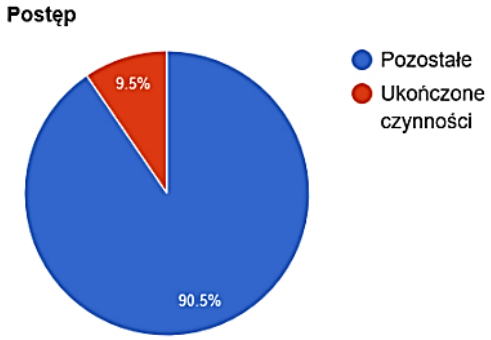
- Narzędzie Diagrams.net [4] − darmowe rozwiązanie opracowane przez JGraph Ltd., które umożliwia tworzenie diagramów między innymi typu UML, sieciowego czy schematów blokowych.
- Narzędzie SQL Server Management Studio − środowisko opracowane przez firmę Microsoft, które między innymi umożliwia dostęp, konfigurowanie oraz administrowanie komponentami SQL Server, Azure SQL Database oraz Azure Synapse Analytics.

Do implementacji projektu zostało wybrane Microsoft Visual Studio wersja 2019. Typem projektu jest aplikacja webowa w architekturze klient-server oparta na technologii ASP.NET Core. Językiem dominującym jest C# oraz cshtml (składnia Razor) wraz ze wstawkami w języku Java Script. Na etapie implementacji ZTA Migration App narzędzie to służyło do konfigurowania oraz administrowania komponentami bazy danych Azure o nazwie ZTADB. Umożliwiło ono również testowanie zapytań do bazy oraz odpowiednie ustawienie parametrów tabel.

Do zarządzania procesem projektowania wykorzystano Git [16]. To darmowe oprogramowanie umożliwia przechowywanie zarówno małych, jak i dużych projektów, kontrolę wersji wytworzonego projektu oraz równoległą pracę nad funkcjonalnościami poprzez tak zwane gałęzie (ang. branch). W trakcie implementacji narzędzia ZTA Migration App zostało utworzone repozytorium [8] o nazwie ZTA. Ostateczna wersja znajduje się na gałęzi master. Narzędzie to było pomocne przy kontroli wersji oprogramowania oraz przywracania zmian.

Nazwa systemu: ZTA Migration App Data rozpoczęcia: 01/08/2022 08:44
Data zakończenia: 01/08/2022 08:49

Imię i nazwisko pracownika: Weronik Buras ID: 24
Komentarz: Brak zastrzezen poza punktem 1



Numer	Czynność	Komenatrz	Data zakończenia
1	1. Sprawdź, czy jest zatwierdzona lista zasobów w sieci przedsiębiorstwa. Jeśli tak wykonaj czynność z punktu 2, w przeciwnym wypadku wykonaj czynność z punktu 1.1 1.1. a. Przeanalizuj źródła danych dostępnych w przedsiębiorstwie oraz usługi. b. Wyznacz te z nich, które będą uznawana za zasoby. c. Zapisz wyznaczone zasoby w dokumencie polityki. d. Udostępnij dokument zgodnie z polityką bezpieczeństwa w przedsiębiorstwie.	Po konsultacji z Basia Adamczyk	02/05/2021 03:10

Rys. 5. Fragment raportu wygenerowanego przy użyciu html2pdf.js

Creative-tim [14] jest witryną, która wspomaga tworzenie interfejsu graficznego. Stanowi ona również swojego rodzaju repozytorium, zawierające udostępnione przez twórców szablony stron w formie płatnej lub darmowej w danych kategoriach np. blog, pulpit użytkownika czy aplikacji. Do implementacji ZTA Migration App użyto szablonu [15] w wersji standardowej, który składał się z plików html zawierających fragmenty Java Script. Zostały wykorzystane klasy css, w celu nadania elementom odpowiedniego wyglądu oraz

fragmenty funkcji Java Script. Narzędzie zostało użyte jedynie w tak zwanym Front-Endzie[2].

W ZTA Migration App został użyty, w celu wygenerowania zestawienia zakończonych i nadal wypełnianych instancji roboczych procedur oraz postępu w ich wypełnianiu, Google Chart firmy Google. Przykładowy wykres jest przedstawiony na rysunku 5 wraz z fragmentem raportu.

Do generowania raportu w formacie .pdf została wykorzystana biblioteka Html2pdf.js [7] w formie wstawki w języku Java Script. Wynikiem jest plik zawierający informacje o użytkowniku (wykonującym procedurę migracji), dacie zakończenia i rozpoczęcia migracji, wykres postępów oraz tabela z listą czynności, komentarzem oraz datą i godziną wykonania danej czynności.

Do uruchamiania aplikacji w fazie jej implementacji używana była przeglądarka internetowa Mozilla Firefox [21] w wersji 95.0.2.

6. Podsumowanie

Migracja do architektury Zero Trust pojawiła się w ofertach wielu znanych firm, takich jak np.: Microsoft [20], IBM [18], Vmware [24] czy cirtix [5] – rozwiązanie to zyskuje na popularności. ZTA Migration App jest narzędziem, które z powodzeniem może zostać użyte w większych oraz mniejszych przedsiębiorstwach do wspomagania takiej migracji. Poprzez hierarchię ról ułatwia zarządzanie użytkownikami oraz kontrolę nad wykonywanymi działaniami. Ponadto nie wymaga instalacji, a jedynie dostępu do Internetu oraz zainstalowanej przeglądarki.

Oczywiście narzędzie ZTA Migration App nie jest doskonałe. Można wprowadzić do niego dużo ulepszeń, takich jak dodatkowe wersje językowe, rozszerzenie o wspomaganie oceny jakości migracji itd. Wydaje się jednak, że w związku z rosnącym poziomem świadomości istotności bezpieczeństwa systemów informacyjnych oraz zwiększającej się popularności tematyki Zero Trust, zaprezentowane w tym artykule narzędzie, pomimo wskazanych niedoskonałości, może być przydatne.

Należy zwrócić również uwagę na praktyczne wykorzystanie Narodowych Standardów Cyberbezpieczeństwa (NSC), które są odpowiednikami standardów amerykańskich przetłumaczonymi na język polski. Celem powstania NSC było między innymi podniesienie poziomu odporności systemów informacyjnych

[2] Front-End – określa wygląd systemu, odpowiada za interakcję klienta z oprogramowaniem, ale nie za jego funkcjonowanie. Przekazuje również dane pobrane od użytkownika i wyświetla otrzymane wartości. Opisany w publikacji [23].

administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania incydentom i reagowania na nie oraz rozwój krajowego systemu cyberbezpieczeństwa [25]. Wiele istotnych błędów oraz wad zauważyła jedna z Europe's Top Cyber Women Joanna Karczewska [26]. Przetłumaczone standardy zwierają wiele błędów spowodowanych tłumaczeniem – niedoprecyzowanym lub sugerującym czytelnikowi inne znaczenie. Ponadto wiele z nich jest zapisanych w nieczytelny i nieklarowny sposób. Można również zauważyć brak odniesienia do rozporządzenia o Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Niewątpliwie opracowane standardy wymagają wielu zmian oraz poprawek i ujednolicenia, aby mogły być używane właściwie oraz z oczekiwanym skutkiem. Na ten moment wydaje się jednak, iż mimo ponownie zgłoszonego problemu przez Panią Joannę Karczewską również na posiedzeniu Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii [27], nie zostaną poczynione żadne działania, aby poprawić i ujednolicić zaistniałe rozbieżności oraz błędy. Obecnie, biorąc pod uwagę często wysoki poziom skomplikowania standardów, właściwym wyborem pomiędzy polską a angielską wersją danego standardu wydaje się oryginalna wersja w języku angielskim, która może zminimalizować możliwość wystąpienia niezrozumienia lub niedoprecyzowania.

Literatura

[1] Buras W., *Narzędzie do wspomagania migracji systemów informacyjnych do „Zero Trust Architecture"*. Praca dyplomowa, WAT, Warszawa, 2022.

[2] Liderman K., *Bezpieczeństwo Informacyjne, Nowe Wyzwania*. PWN, Warszawa, 2017.

Źródła elektroniczne

[3] https://r.uek.krakow.pl/bitstream/123456789/2265/1/164782050.pdf (dostęp 22.12.2022).

[4] https://app.diagrams.net/ (dostęp 10.11.2021).

[5] https://citrixready.citrix.com/program/workspace-security-program.html (dostęp 07.04.2022).

[6] https://csrc.nist.gov/publications/detail/sp/800-207/final (dostęp 07.04.2022).

[7] https://ekoopmans.github.io/html2pdf.js/?fbclid=IwAR3mv5Sv2isMd5zrCqhxfn_OqYoD9lD6awsTWkBq1XnVe_gy2ThZLQle1AM (dostęp 20.11.2021).

[8] https://github.com/sloiczek7714/ZTA (dostęp 09.04.2022).

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (dostęp 07.04.2022).

[10] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRIEi?culture=pl-pl&country=PL (dostęp 30.03.2022).

[11] https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/ (dostęp 30.03.2022).

[12] https://thebossmagazine.com/zero-trust-cybersecurity/ (dostęp 30.03.2022).

[13] https://thehacksummit.com/ (dostęp 20.03.2022).

[14] https://www.creative-tim.com/ (dostęp 15.12.2021).

[15] https://www.creative-tim.com/product/material-dashboard-dark (dostęp 15.12.2021).

[16] https://www.git-scm.com/ (dostęp 10.11.2021).

[17] https://www.gov.pl/attachment/8659d8de-6a83-4860-bcd1-d0648fbe9ead (dostęp 07.04.2022).

[18] https://www.ibm.com/pl-pl/security/zero-trust (dostęp 07.04.2022).

[19] https://www.isaca.org/resources/news-and-trends/industry-news/2020/harnessing-zero-trust-security (dostęp 30.03.2022).

[20] https://www.microsoft.com/pl-pl/security/business/zero-trust (dostęp 07.04.2022).

[21] https://www.mozilla.org/pl/firefox/new/

[22] https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture (dostęp 30.03.2022).

[23] https://www.pluralsight.com/blog/software-development/front-end-vs-back-end (dostęp 20.11.2021).

[24] https://www.vmware.com/solutions/zero-trust-security.html (dostęp 07.04.2022).

[25] https://www.wojsko-polskie.pl/aszwoj/u/93/94/9394db01-d323-4635-b798-ac4effa0a822/polska.pdf (dostęp 22.12.2022).

[26] https://portal.pti.org.pl/wp-content/uploads/2022/07/8.-Cyberbezpieczenstwo-po-amerykansku_Domena_1-2022.pdf (dostęp 22.12.2022).

[27] https://www.sejm.gov.pl/sejm9.nsf/biuletyn.xsp?documentId=ED74121743CB0FBDC125888300450187 (dostęp 22.12.2022).

Tool for supporting the migration of organizational information systems to „Zero Trust Architecture”

ABSTRACT: The paper presents basic information on the „Zero Trust Architecture” concept and a project involving a tool designed to support the migration of information systems to this architecture. Initially, the Zero Trust concept is briefly described, followed by the presentation of steps based on NSC 800-207 necessary for migrating information systems to this architecture. Subsequently, the procedure for practically using this list is outlined. Finally, the implementation of this procedure into a migration support tool is described.

KEYWORDS: Zero Trust Architecture, information systems, security of information systems, NIST 800-207, NIST SP 800-207

Praca wpłynęła do redakcji: 11.04.2022 r.

Analiza ryzyka na potrzeby bezpieczeństwa informacyjnego według zaleceń normy PN-ISO/IEC 27005

Krzysztof LIDERMAN

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono podstawy formalne oszacowania ryzyka IT metodą jakościową zgodną z wytycznymi zawartymi w normie PN-ISO/IEC 27005:2014-01. Ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych.

SŁOWA KLUCZOWE: bezpieczeństwo informacyjne, norma PN-ISO/IEC 27005, oszacowanie ryzyka IT

Ekspert „od ryzyka”:
osoba, która wykonuje precyzyjne zgadywanie na podstawie niewiarygodnych danych dostarczonych przez osoby o wątpliwej wiedzy.

definicja „z Internetu”

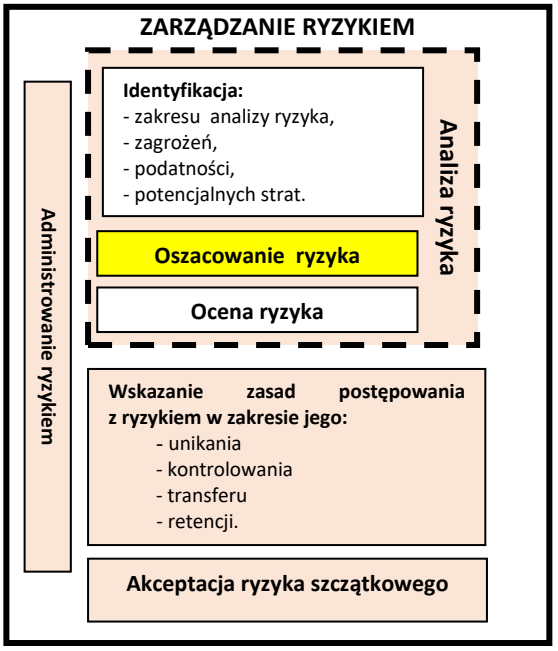
1. Wprowadzenie

Zarządzanie ryzykiem jest to systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka[1]. Podstawowe elementy tego procesu można przedstawić w formie graficznej jak na rys. 1. Żeby spełnić formalne wymagania

[1] Definicja za PN-IEC 62198 [3].

definicji zarządzania, jakość realizacji wymienionych w niej zadań powinna być mierzalna, a cały proces powinien układać się w cykl Deminga.

Pierwszym podstawowym elementem procesu zarządzania ryzykiem jest (pod)proces analizy ryzyka. Kluczowym zadaniem tego podprocesu jest wyznaczanie wartości ryzyka i to zagadnienie jest opisane w tym artykule. Opis jest skonkretyzowany na ryzyko IT, gdzie ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych.



Rys. 1. Podstawowe elementy zarządzania ryzykiem

Obecnie nie tylko w Polsce, ale i na świecie, w zakresie analizy ryzyka IT zaleca się przeprowadzanie jej zgodnie z wytycznymi normy ISO/IEC 27005. Na przykład w Polsce wykonywanie analizy ryzyka według wytycznych normy PN-ISO/IEC 27005 dla systemów IT eksploatowanych w podmiotach administracji publicznej narzuca rozporządzenie: *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[2], w którym okresową analizę ryzyka nakazuje punkt 3 ustępu 2 paragrafu 20:

[2] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów*

§20.1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

(…)

3) **przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji** oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Natomiast w ustępie 3 ww. paragrafu stwierdza się:

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) **PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem**;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W proces zarządzania ryzykiem są zaangażowane role, których nazwy są zwykle podawane w literaturze przedmiotu i praktyce korporacyjnej w postaci anglojęzycznych akronimów:

- CISO (ang. *Chief Information Security Officer*) – rola do nadzoru i kontroli realizacji przyjętych w {Podmiot}[3] zasad bezpieczeństwa oraz do podejmowania decyzji w sprawach określonych zapisami Polityki Bezpieczeństwa Informacji.

publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; Dz. U. 2012 poz. 526;
(źródło: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20120000526).

[3] Dalej w artykule jako ogólną nazwę organizacji, dla której jest przeprowadzana analiza ryzyka, przyjęto słowo „Podmiot", ujęte w nawiasy klamrowe. W przypadku konkretyzacji zapisów metodyki ALR-27005, w to miejsce należy wpisać nazwę organizacji (np. Wojskowa Akademia Techniczna) bądź jej symbol (np. WAT).

- CRO (ang. *Chief Risk Officer*) – rola uprawniająca do akceptacji ryzyka.
- CTO (ang. *Chief Technical Officer*) – rola właściciela ryzyka IT.

W dalszej części artykułu jest przedstawiony zarys propozycji czteroetapowej metodyki analizy ryzyka IT, o nazwie ARL-27005, w której wykorzystuje się jakościową metodę oszacowania wartości ryzyka w sposób zalecany w normie PN-ISO/IEC 27005:2014[4]. W metodyce określono czynności analizy, wskazano role odpowiedzialne za wykonanie danych czynności, zaproponowano wzorce zapisu wyników czynności.

Przyjęto, że każde zagrożenie można przypisać do jednej z trzech klas:

- „Siły wyższe" − oznaczane dalej symbolem **SW**. Należą do nich wszystkie zdarzenia, na które uprawniony podmiot − dysponent lub właściciel systemu teleinformatycznego albo zasobu informacyjnego, nie ma wpływu. Do zdarzeń takich należą katastrofy naturalne, promieniowanie kosmiczne, emisja ujawniająca itp.
- Celowe działanie wrogiego podmiotu − oznaczane dalej symbolem **CE**. Wrogi podmiot może być indywidualny (typu „samotny haker") lub grupowy (np. grupa przestępcza typu APT).
- Błędne działanie uprawnionego podmiotu − oznaczane dalej symbolem **BŁ**. Uprawnionym podmiotem jest zwykle pracownik konkretnej organizacji {Podmiot}.

2. Metodyka ARL-27005[5]

ETAP I: IDENTYFIKACJE

1) Zidentyfikować (odpowiedzialny – CTO):
   - zasoby poddawane analizie,
   - procesy poddawane analizie,

[4] W analizie ryzyka IT powinny być wykorzystane, w razie potrzeby, informacje z Rejestru Ryzyka {Podmiot}, a wyniki analizy powinny być w tym Rejestrze zapisane.

[5] Metodyka została przygotowana na podstawie zapisów normy PN-ISO/IEC 27005:2014. Norma ta została przez Polski Komitet Normalizacyjny (PKN) wycofana 12.10.2021. Najnowsza oryginalna wersja tej normy to ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*, wprowadzona 25.10.2022 r. Zastąpiła ona wydanie z roku 2018. W chwili pisania tego artykułu nie są znane zamierzenia PKN w sprawie wydania normy polskiej. Warto zauważyć, że Narodowe Standardy Cyberbezpieczeństwa za podstawę w dziedzinie zarządzania ryzykiem mają standardy NIST (NSC-800-30 wer.1.0, NSC-800-37 wer.1.0, NSC-800-39 wer.1.0; dostęp 05.11.2022) a nie ISO/IEC.

- usługi poddawane analizie.

Wynikiem identyfikacji powinny być wstępnie wypełnione tabele 1-3.

2) Wstępnie zidentyfikować (odpowiedzialny – CTO) zagrożenia[6] istotne dla działalności biznesowej Podmiotu. Wynikiem identyfikacji powinna być wstępnie wypełniona tabela 4.
3) Metodą „burzy mózgów" (patrz np. [1] rozdz. 3.4.3) uzupełnić tabele 1-4.

ETAPII: SZACOWANIE RYZYKA

Wykonać procedurę opisaną w rozdziale 3.

ETAP III: OCENA RYZYKA

Uszeregować otrzymane wartości zmiennych $RYZYKO_{dzjpz}$ według wielkości. Analogicznie, w razie potrzeby, uszeregować wartości zmiennych $RYZYKO_{dpjpz}$ dla procesów. Czynności wykonywane w tym punkcie składają się na **proces oceny ryzyka**.

Tab. 1. Wzorzec arkusza opisu zasobu (przykład)

ARKUSZ nr ……. OPISU ZASOBU	
Typ zasobu: [infrastrukturalny, teleinformatyczny, informacyjny, systemu ochrony]	
Identyfikator zasobu: [symbol identyfikacyjny]	
Opis zasobu:	[krótki opis zasobu]
Umiejscowienie zasobu:	[wskazanie fizycznej lokalizacji zasobu; wskazanie numeru schematu, na którym jest zaznaczony]
Właściciel zasobu:	[dane właściciela zasobu: stanowisko, telefon]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju zasobu:	np. dla zasobu typu teleinformatycznego (komputer): jaki producent, jaki dostawca, jaki okres eksploatacji, gdzie pliki konfiguracyjne itp.

[6] Należy rozróżniać zagrożenie $\delta_k \in \Delta$ od sposobu jego realizacji $\delta|d_n \in D$. Szczegóły – patrz rozdz. 3.1.

Tab. 2. Wzorzec arkusza opisu procesu (przykład)

ARKUSZ nr ……. OPISU PROCESU	
Typ procesu: [krytyczny, kluczowy, wspomagający]	
Identyfikator procesu: [symbol identyfikacyjny]	
Opis procesu:	[krótki opis procesu]
System IT realizujący proces:	[wskazanie systemu IT, w którym proces jest realizowany i wykorzystywane zasoby]
Właściciel procesu:	[dane właściciela procesu: stanowisko, telefon]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju procesu:	np. powiązanie z innymi procesami itp.

Tab. 3. Wzorzec arkusza opisu usługi (przykład)

ARKUSZ nr ……. OPISU USŁUGI	
Typ usługi: [wewnętrzna, zewnętrzna]	
Identyfikator usługi: [symbol identyfikacyjny]	
Opis usługi:	[krótki opis usługi]
Klient/wykonawca usługi:	[wskazanie nazw i kontaktów]
Dane o umowie:	[dane nt. umowy na świadczenie usługi: symbole identyfikacyjne, gdzie jest przechowywana, okres obowiązywania]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju usługi:	np. powiązanie z innymi usługami, wykorzystywane procesy i zasoby itp.

Tab. 4. Wzorzec arkusza opisu zagrożenia i sposobu jego realizacji (przykład)

ARKUSZ nr ……. OPISU ZAGROŻENIA	
Identyfikator zagrożenia: [symbol zagrożenia: SW – „siły wyższe”; CE – działania celowe; BŁ – działania błędne]	
Zagrożenie:	[jednozdaniowa nazwa opisowa zagrożenia]
Scenariusz realizacji zagrożenia dla:	[**Poufności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Integralności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Dostępności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Rozliczalności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY]
Zasoby, na które zagrożenie może mieć wpływ i szkody:	[lista: zasób/szkoda/właściciel zasobu]
Procesy, na które zagrożenie może mieć wpływ i szkody:	[lista: proces/szkoda/właściciel procesu]
Usługi, na które zagrożenie może mieć wpływ i szkody:	[lista: usługa/szkoda/symbole identyfikacyjne umowy]
Potencjał zagrożenia:	[kilkuzdaniowy opis słowny]

ETAP IV: AKCEPTACJI RYZYKA

1) Ustalić, jakie wartości ryzyka są akceptowane w {Podmiot}. Ponieważ na wartość ryzyka składają się dwa elementy – prawdopodobieństwo (możliwość) zajścia incydentu (MZI) oraz wielkość szkód (ST) – **należy odnieść się do obu tych elementów**[7], inaczej wskazanie wartości ryzyka będzie nieprecyzyjne. Przyjmuje się, że wartości ryzyka równe lub poniżej wartości akceptowalnych oznaczają **ryzyko akceptowalne**, wobec którego (w zasadzie) nie podejmuje się działań minimalizujących.

[7] Na przykład (tabela 7): akceptujemy tylko zdarzenia (incydenty), których możliwość zajścia jest co najwyżej na poziomie „średni”, a ich skutki nie mogą być większe niż „niskie”. Taka decyzja wskazuje konkretne ryzyko o wartości 2. Widać, że jest jeszcze jedno ryzyko o wartości 2, ale nie spełnia warunków akceptacji – możliwość zajścia jest na poziomie „niski”, ale skutki mają wartość „średnie”.

2) Uzyskać od CRO zatwierdzenie ryzyka akceptowalnego.
3) Dla ryzyka o wartościach **nieakceptowanych** wykonać czynności z kolejnego etapu zarządzania ryzykiem, tj. etapu minimalizowania ryzyka (poza niniejszą metodyką).

3. Procedura szacowania ryzyka IT

3.1. Założenia

- dany jest zbiór zagrożeń Δ takich, że $\delta_k \in \Delta$, gdzie δ_k jest konkretnym, zidentyfikowanym zagrożeniem dotyczącym zasobu $z_i \in Z$ (lub, analogicznie, procesu $p_j \in P$), podlegającemu analizie ryzyka;
- dany jest zasób $z_i \in Z$, gdzie Z to zbiór zasobów oraz proces $p_j \in P$, podlegające analizie ryzyka;
- z_i może mieć podatności $pz_{zi} \in PZ_z$, gdzie PZ_z to podzbiór podatności zasobów należących do zbioru Z. Podobnie, proces p_j może mieć podatności $pz_{pi} \in PZ_p$, gdzie PZ_p to podzbiór podatności procesów należących do zbioru P;
- podatność może być wykorzystana przez zagrożenie $\delta | d_n \in D$, gdzie D to zbiór zidentyfikowanych sposobów d_n realizacji zagrożeń mogących oddziaływać na zasoby Z lub procesy P;
- analiza ryzyka jest przeprowadzona w wariancie zasobowym lub procesowym (w zależności od konkretnych potrzeb);
- w oszacowaniach wykorzystuje się oceny opisowe (czyli analiza ryzyka jest przeprowadzana tzw. metodą jakościową).

Należy określić:

1) Jednolite oceny symboliczne[8] dla cech (zmiennych): zagrożeń δ_k i sposobów ich realizacji $d_n \in D$, podatności $p_j \in P$, szkód i strat oraz ryzyka. Te cechy to:
   - możliwość realizacji zagrożenia, oznaczona dalej jako MRZ,
   - stopień podatności, oznaczony dalej jako PZ,
   - możliwość zajścia incydentu (tj. poniesienia szkód spowodowanych realizacją określonego zagrożenia), oznaczona dalej jako MZI,
   - wielkość szkód, oznaczona dalej jako ST,
   - wielkość ryzyka, oznaczona dalej jako RYZYKO.

[8] Tak będą nazywane miary w szacowaniach jakościowych w odróżnieniu od miar liczbowych (miar prawdopodobieństwa, tj. liczb z przedziału [0,1]) w przypadku oszacowań ilościowych. Miary symboliczne mogą być opisowe (np. wysoki, średni, niski) lub w postaci liczb (ilości punktów, zakresów przedziałów itd.).

2) Sposób wyznaczania ocen.

Przyjmuje się następujący system K przypisywania ocen opisowych wybranym cechom:

$$K = \langle CECHA, OCENA, PROCEDURA \rangle$$

gdzie:

– CECHA – zbiór cech (zmiennych) {MRZ, PZ, MZI, ST, RYZYKO}.

– OCENA – zbiór ocen opisowych {K, W, S, N} gdzie[9]:

K – prawdopodobieństwo (możliwość), stopień lub szkoda KRYTYCZNA,

W – prawdopodobieństwo (możliwość), stopień lub szkoda WYSOKA,

S – prawdopodobieństwo (możliwość), stopień lub szkoda ŚREDNIA,

N – prawdopodobieństwo (możliwość), stopień lub szkoda NISKA.

Ten zbiór ocen opisowych jest odwzorowywany na przyjęty arbitralnie czteroelementowy zbiór liczb naturalnych:

$$\{K, W, S, N\} \rightarrow \{4, 3, 2, 1\} \quad (1)$$

co ilustruje tabela 5.

Tab. 5. Odwzorowanie ocen opisowych w czteroelementowy zbiór liczb

Prawdopodobieństwo realizacji zagrożenia (MRZ)	**Podatność (PZ)**	**Szkody (ST)**	**Wartość liczbowa**	
Niskie	Niska	Niskie	**1**	
Średnie	Średnia	Średnie	**2**	
Wysokie	Wysoka	Wysokie	**3**	
Prawie pewne	Krytyczna	Krytyczne	**4**	

– PROCEDURA – podaje sposób przypisania wartości ocen opisowych ze zbioru OCENA cechom ze zbioru CECHA (np. decyzją ekspertów w ramach sesji „burzy mózgów” – patrz np. [1] rozdz. 3.4.3).

[9] Ten zbiór ocen został w tym artykule przyjęty arbitralnie, w celu zachowania zgodności z propozycjami zawartymi w normie PN-ISO/IEC 27005. W ogólnym przypadku zbiór ten może być dowolny zarówno co do liczności, jak i nazw.

3.2. Podstawowe czynności formalne procesu szacowania ryzyka

W celu oszacowania ryzyka powstania strat określonej wielkości, **dla zasobu** $z_i \in Z$ (gdzie Z to zbiór zasobów podlegających analizie ryzyka), **konkretnego zagrożenia δ** oraz **sposobu jego realizacji** $d_n \in D$ i **podatności** $pz_j \in PZ_z$, należy[10]:

1) Dla $d_n \in D$ oszacować prawdopodobieństwo (możliwość) MRZ realizacji zagrożenia δ_k „jako takiego”[11], tzn. podać wartość: ocena(MRZ_d). Na przykład, gdy oceniono prawdopodobieństwo realizacji zagrożenia δ_k w sposób d_n jako „wysoką”, otrzymuje się: ocena(MRZ_d)=W.
2) Oszacować stopień podatności $pz_{zj} \in PZ_z$ zasobu $z_i \in Z$, która to podatność może być wykorzystana przez zagrożenie (jedno lub więcej), tzn. podać wartość: ocena(PZ_z).
3) Wykonać odwzorowanie według formuły (1):

$$\text{ocena}(MRZ_d) \rightarrow \{4, 3, 2, 1\}$$
$$\text{ocena}(PZ_z) \rightarrow \{4, 3, 2, 1\}$$

4) Oszacować według formuły (2) prawdopodobieństwo (możliwość) MZI_{dpz} zajścia incydentu (dokładniej: zajścia zdarzenia takiego, że zagrożenie δ_k w sposób $d_n \in D$ wykorzysta podatność $pz_{zj} \in PZ_z$ do spowodowania szkody):

$$\text{ocena}(MZI_{dpz}) = \text{ocena}(MRZ_d) \times \text{ocena}(PZ_z) \quad (2)$$

gdzie × oznacza arytmetyczną operację mnożenia.

5) Oszacować wielkość szkód $st_{zj} \in ST$ dla zasobu $z_i \in Z$, powstałych w wyniku realizacji zagrożenia δ_k w sposób d_n; tzn. podać wartość: ocena(ST_{dzj}).
6) Wykonać odwzorowanie według formuły (1):

$$\text{ocena}(ST_{dzj}) \rightarrow \{4, 3, 2, 1\}$$

7) Oszacować według formuły (3) ryzyko; dokładniej: zajścia zdarzenia takiego, że zagrożenie δ_k wykorzysta w sposób $d_n \in D$ podatność $p_{zj} \in PZ_z$ do

[10] Dalej proces szacowania ryzyka będzie pokazany tylko dla zasobu, ponieważ dla procesów ze zbioru P wykonuje się go analogicznie.

[11] Na tym etapie szacujemy „potencjalność” zagrożenia. Np. oceniając możliwość kradzieży sprzętu komputerowego z siedziby organizacji nie bierzemy pod uwagę krat, zamków, systemów alarmowych itp. w które wyposażony jest budynek (to wpływa na podatność na kradzież, co rozpatrywane jest w kolejnym etapie) tylko bierzemy pod uwagę to, że budynek ten znajduje się w dzielnicy w której mieszka dużo złodziei (podobno „prawdziwi” złodzieje na swoim terenie nie kradną, ale czasy się zmieniają).

spowodowania szkody, a wielkość poniesionych strat będzie miała wartość: ocena(ST_{dzj}):

$$\text{ocena}(RYZYKO_{dzjpz}) = \text{ocena}(MZI_{dpz}) \times \text{ocena}(ST_{dzj}) \qquad (3)$$

Zbiory wartości liczbowych ocen możliwych do uzyskania przez zmienne MZI oraz RYZYKO ilustrują tabele 6 i 7.

Używając przyjętych ocen opisowych, można wskazać zmienną o jakiej wartości liczbowej wypadkowej przypisać do jakiej oceny opisowej ze zbioru {K, W, S, N}. **Założenie:** oceną opisową (wypadkową) jest ocena wyższa z dwóch składowych, czyli ma zastosowanie formuła max{OCENA}.

W tabelach 6 i 7 uzyskane wyniki zastosowania formuły max{OCENA} są podane w nawiasach okrągłych. W tabeli 7 obok ocen liczbowych wypadkowych podane są zbiory ocen opisowych {MRZ, PZ} sprzyjających zajściu zdarzenia (w tym przypadku − incydentu) o konkretnej wartości liczbowej. Informacja ta jest istotna, ponieważ wskazuje, po identyfikacji konkretnych wartości MRZ i PZ, jakie istnieją możliwości minimalizowania ryzyka, czyli jakie są możliwości oddziaływania na składowe ryzyka.

Stosując podaną zasadę do zbioru {MZI, ST}, można określić przyporządkowanie uzyskanych wartości ryzyka do zbioru ocen opisowych (patrz tabela 6 − wartości opisowe są podane w nawiasach okrągłych).

Uwaga: podanych wartości ocen opisowych ryzyka **nie należy utożsamiać z ryzykiem akceptowalnym lub nieakceptowanym**. To, jakie ryzyko o jakiej wartości jest ryzykiem akceptowalnym, jest decyzją właściciela ryzyka lub osoby uprawnionej do takiej decyzji. W {Podmiot} osobą uprawnioną jest osoba pełniąca rolę CRO; progi akceptacji („apetyt na ryzyko") określa Zarząd {Podmiot}.

Tab. 6. Wartości ocen dla MZI (szare pole)

PZ \ MRZ	1	2	3	4
1	1 (N)	2 (S)	3 (W)	4 (K)
2	2 (S)	4 (S)	6 (W)	8 (K)
3	3 (W)	6 (W)	9 (W)	12 (K)
4	4 (K)	8 (K)	12 (K)	16 (K)

Tab. 7. Wartości ocen dla RYZYKA (szare pole)[12]

ST / MZI	1	2	3	4
1	**1** (N) {N, N}	**2** (S) {N, S}	**3** (W) {N, W}	**4** (K) {N, K}
2	**2** (S) {S, N} {N, S} {S, S}	**4** (S) {S, N} {N, S} {S, S}	**6** (W) {S, N} {N, S} {S, S}	**8** (K) {S, N} {N, S} {S, S}
3	**3** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**6** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**9** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**12** (K) {W, N} {N, W} {S, W} {W, S} {W,W}
4	**4** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**8** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**12** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**16** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}

8) Czynności 1-7 powtórzyć:
   a) dla każdego zidentyfikowanego sposobu realizacji d_n zagrożenia δ_k na zasobie z_i;
   b) czynność a) powtarzać dla kolejnych zagrożeń ze zbioru Δ i sposobów realizacji ze zbioru D, aż do wyczerpania zagrożeń i sposobów ich realizacji na zasobie z_i;
   c) dla kolejnego zasobu ze zbioru Z wykonać czynności z punktu 8a i b aż do wyczerpania zbioru Z;
   d) w razie potrzeby wykonać analogiczne czynności dla zbioru procesów P poddawanych analizie ryzyka.
9) Wynikiem realizacji czynności z punktu 8 powinny być wypełnione tabele 8-11:

[12] W szarych polach, w nawiasach okrągłych, podana jest ocena opisowa wartości ryzyka. W nawiasach klamrowych są podane zdarzenia ({MRZ, PZ} – patrz tabela 6) sprzyjające zaistnieniu ryzyka o tej wartości.

Tab. 8. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu POUFNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_{PF}$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_{PF}, CE_{PF}, $BŁ_{PF}$}	PZ_{SWPF} ( ) PZ_{CEPF} ( ) $PZ_{BŁPF}$ ( )			

Opis podatności:

$PZ1_{SWPF}$ ( )
$PZ2_{SWPF}$ ( )
...
$PZ1_{CEPF}$ ( )
$PZ2_{CEPF}$ ( )
…
$PZ1_{BŁPF}$ ( )
$PZ2_{BŁPF}$ ( )
...

Uwaga: podatność całkowitą PZ_{XXPF} na konkretną realizację zagrożenia ustala się, analizując zidentyfikowane podatności cząstkowe (opisane pod tabelą jako: $PZ1_{SWPF}$ ( ), $PZ2_{SWPF}$ ( ), …).

Tab. 9. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu INTEGRALNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ]× [PZ]	**STRATY** [ST]	**RYZYKO$_I$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_I, CE_I, $BŁ_I$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWI}$ ( )
$PZ2_{SWI}$ ( )
...
$PZ1_{CEI}$ ( )
$PZ2_{CEI}$ ( )

…

$PZ1_{BŁI}$ ( )

$PZ2_{BŁI}$ ( )

...

Tab. 10. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_D, CE_D, $BŁ_D$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWD}$ ( )

$PZ2_{SWD}$ ( )

...

$PZ1_{CED}$ ( )

$PZ2_{CED}$ ( )

…

$PZ1_{BŁD}$ ( )

$PZ2_{BŁD}$ ( )

...

Tab. 11. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu ROZLICZALNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_R$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_R, CE_R, $BŁ_R$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWR}$ ( )

$PZ2_{SWR}$ ( )

...

$PZ1_{CER}$ ( )

$PZ2_{CER}$ ( )

…

$PZ1_{BŁR}$ ( )

$PZ2_{BŁR}$ ( )

...

Uwaga! Dla procesów i usług należy utworzyć i wypełnić tabele analogiczne jak dla zasobu (tj. na wzór tabel 8-11).

4. Podsumowanie

W artykule przedstawiono sposób szacowania wartości ryzyka zgodny z zaleceniami normy PN-ISO/IEC 27005. W normie zaleca się użycie metody jakościowej[13] z wykorzystaniem wartości liczbowych. W praktyce oceny do analizy ryzyka tą metoda pozyskuje się zwykle od ekspertów, którzy swoje opinie wyrażają jednak w sposób opisowy słowny, a nie liczbowy, posługując się takimi stwierdzeniami, jak: wysoki, krytyczny, możliwy, nieprawdopodobny, niski itp. Metoda zamieszczona w normie zakłada przekształcenie takich ocen na liczby i dalsze działania na tak przekształconych ocenach opisowych.

Zdaniem piszącego te słowa, przypomina to sięganie prawą ręką do lewej kieszeni spodni − prościej byłoby działać bezpośrednio na słownych ocenach opisowych przedstawionych przez ekspertów. Przykłady takiej metody są zamieszczone w rozdz. 3 w pracy [1] i w artykule [2].

Przykłady zastosowania przedstawionej w tym opracowaniu metodyki zostaną zaprezentowane w kolejnym artykule.

Literatura

[1] LIDERMAN K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN Warszawa, 2017.

[2] LIDERMAN K., *Risk of undesired changes to significant information quality criteria*, Teleinformatics Review, Nr 3-4(47), WAT, Warszawa 2019, pp. 31-55.

[3] PN-IEC 62198:2005, *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania*.

[4] PN-ISO/IEC 27005:2014, *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

[13] Taka jest ogólnie przyjęta nazwa tej metody, chociaż trafniejsza byłaby nazwa „metoda ocen opisowych”.

[5] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, Dz. U. 2012 Nr 0 poz. 526.

Risk analysis for information security in accordance with PN-ISO/IEC 27005 recommendation

ABSTRACT: The paper considers the problem of IT risk evaluation with the use of a quality method based on the PN-ISO/IEC 27005:2014-01 recommendation. It addresses risks associated with the realization of threats that result in damages to telecommunications systems and processed information resources.

KEYWORDS: information security, PN-ISO/IEC 27005, IT risk evaluation

Praca wpłynęła do redakcji: 23.11.2022 r.

Oszacowania ryzyka IT – studium przypadków

Krzysztof LIDERMAN

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono na trzech przykładach sposób oszacowania ryzyka IT. Ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych. Prezentowane w przykładach oszacowanie ryzyka jest wykonane metodą jakościową, z użyciem czterech ocen opisowych „przekładanych" na wartości liczbowe zgodnie z wytycznymi zawartymi w normie PN-ISO/IEC 27005:2014-01.

SŁOWA KLUCZOWE: bezpieczeństwo informacyjne, realizacja zagrożenia, oszacowanie ryzyka IT

1. Wprowadzenie

Zagrożenia[1] dla systemów teleinformatycznych (IT) oraz zasobów informacyjnych w nich przetwarzanych, można sklasyfikować następująco:

1. **„Siły wyższe"** – zdarzenie zewnętrzne, niemożliwe (lub prawie niemożliwe) do przewidzenia, którego skutkom nie można zapobiec[2].
2. **Działania ludzi:**

[1] Od zagrożenia należy odróżniać sposób jego realizacji, które to rozróżnienie będzie konsekwentnie stosowane w dalszej części artykułu.

[2] Do takich zdarzeń należą m.in. tzw. katastrofy naturalne (trzęsienia ziemi, powodzie itp.), zjawiska przyrodnicze, takie jak emisja ujawniająca oraz zjawiska polityczne, takie jak terroryzm.

2.1. Celowe (nieuprawnione[3] i przestępcze):
   - działania personelu, w tym podsłuchy różnego typu i kradzieże oraz zagubienia nosicieli informacji (sprzętu i dokumentów);
   - działania osób postronnych (klienci, „hakerzy"), w tym różnego typu podsłuchy i kradzieże nosicieli informacji (dokumentów i sprzętu);

2.2. Błędne[4].

Realizacja zagrożeń wpływa niekorzystnie na osiąganie celów biznesowych. COBIT-owe [4] praktyki z zakresu *governance* (EDM03.01: *Ocena, kierowanie, monitorowanie − Zapewnienie optymalizacji ryzyka − Zgodność IT z biznesowymi celami strategicznymi*) wskazują, że zarząd organizacji powinien określić swój „apetyt na ryzyko"[5] i poziom tolerancji ryzyka[6]. Czynniki, które zwiększają poziom ryzyka dla organizacji i jej systemów IT to wrażliwość i objętość przetwarzanych zbiorów danych, krytyczność świadczonych usług, liczba użytkowników, połączenia z siecią publiczną i korzystanie z usług innych podmiotów.

Ogólnie, krytyczność systemów IT jest zależna od wagi ciągłości świadczenia wspieranych procesów biznesowych i usług. Krytyczność systemu może być w praktyce oceniona przez oszacowanie strat finansowych, które mogą wystąpić jako rezultat jego przestoju. Podczas oceny krytyczności systemu jest ważne, aby zrozumieć i uwzględnić wpływ jego przestoju (np. w wyniku awarii) na działanie aplikacji pracujących w stowarzyszonych przepływach biznesowych.

W kolejnych rozdziałach niniejszego artykułu są zaprezentowane trzy przykłady szacowania ryzyka dla różnych zagrożeń i różnych sposobów ich realizacji. Do szacowania ryzyka wykorzystano metodykę opisaną w pracy [3], bazującą na zaleceniach normy PN-ISO/IEC 27005 [6]. W przykładach są wykorzystywane arkusze opisu zasobów oraz arkusze opisu zagrożenia i sposobu jego realizacji, których wzorce przedstawiono w postaci tabel 1 i 2. W przykładach, oprócz rozróżniania zagrożenia i sposobu jego realizacji, są konsekwentnie rozróżniane także szkody i straty.

[3] Działaniami nieuprawnionymi są nazywane takie działania celowe, niepożądane przez dysponenta systemu bądź zasobów danych, które mogą doprowadzić do powstania szkód, ale na które nie ma paragrafów w Kodeksie Karnym („nie wyczerpują ustawowych znamion przestępstwa").

[4] Przykład z 04.10.2021 r. – awaria Facebooka. Powodem awarii była błędna aktualizacja zewnętrznego protokołu trasowania BGP. Specjaliści od sieci Facebooka wprowadzali pewne zmiany w konfiguracji i przez pomyłkę doprowadzili do trwającej kilka godzin awarii.

[5] Czyli poziom ryzyka, który zarząd tej organizacji jest skłonny zaakceptować, aby osiągnąć założone cele biznesowe.

[6] Czyli okresowe, akceptowalne odchylenia od przyjętej wartości „apetytu na ryzyko".

Tab. 1. Wzorzec arkusza opisu zasobu (przykład)

ARKUSZ nr ……. OPISU ZASOBU	
Typ zasobu: [infrastrukturalny, teleinformatyczny, informacyjny, systemu ochrony]	
Identyfikator zasobu: [symbol identyfikacyjny]	
Opis zasobu:	[krótki opis zasobu]
Umiejscowienie zasobu:	[wskazanie fizycznej lokalizacji zasobu; wskazanie numeru schematu, na którym jest zaznaczony]
Właściciel zasobu:	[dane właściciela zasobu: stanowisko, telefon]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju zasobu:	np. dla zasobu typu teleinformatycznego (komputer): jaki producent, jaki dostawca, jaki okres eksploatacji, gdzie pliki konfiguracyjne itp.

Tab. 2. Wzorzec arkusza opisu zagrożenia i sposobu jego realizacji (przykład)

ARKUSZ nr ……. OPISU ZAGROŻENIA	
Identyfikator zagrożenia: [symbol zagrożenia: SW – „siły wyższe”; CE – działania celowe; BŁ – działania błędne]	
Zagrożenie:	[jednozdaniowa nazwa opisowa zagrożenia]
Scenariusz realizacji zagrożenia dla:	[**Poufności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Integralności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Dostępności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Rozliczalności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY]

Zasoby, na które zagrożenie może mieć wpływ i szkody:	[lista: zasób/szkoda/właściciel zasobu]
Procesy, na które zagrożenie może mieć wpływ i szkody:	[lista: proces/szkoda/właściciel procesu]
Usługi, na które zagrożenie może mieć wpływ i szkody:	[lista: usługa/szkoda/symbole identyfikacyjne umowy]
Potencjał zagrożenia:	[kilkuzdaniowy opis słowny]

2. Szacowania ryzyka IT – przypadek 1

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik Sp. z o.o., jest zdarzenie:

ZD_25: Pożar w budynku firmy Płatnik sp. z o.o. przy ul. Moczarowej 3 w Opolu

Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 3.

Tab. 3. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok

Dalej została przedstawiona szczegółowa analiza dla zagrożenia klasy **SW**, realizującego się jako uderzenie pioruna w dach obiektu (zasobu infrastrukturalnego) o identyfikatorze [3/Moczarowa]. Przyjęto, że zdarzenie to nie wpływa na poufność i integralność zasobów informacyjnych. Schemat wykonanej analizy przedstawiony został na rysunku 1.

W celu otrzymania pełnej analizy (i ryzyka) dla zdarzenia:

ZD_25: Pożar w budynku firmy Płatnik sp. z o.o. przy ul. Moczarowej 3 w Opolu

należy przeprowadzić ją także dla:

- zagrożenia klasy **CE,** realizującego się jako podpalenie obiektu [3/Moczarowa] przez zewnętrzny wrogi podmiot;
- zagrożenia klasy **BŁ,** realizującego się jako zaprószenie ognia przez pracownika firmy Płatnik.

ZAGROŻENIE	SPOSÓB REALIZACJI	SKUTEK (INCYDENT)	SZKODA	STRATA	RYZYKO
SW	1(**N**) UDERZENIE PIORUNA $PZ1_{SW}$: brak instalacji odgromowej $PZ2_{SW}$: zła konserwacja instalacji odgromowej 2(**S**) PZn_{SW}:	**POŻAR**	SPALONY DACH MZI=MRZ×PZ= =1×2=2 **MZI_{SW} = S**	95 tys. zł. **2(S)**	2 ×2=**4** **RYZYKO=S**
CE	1(**N**) PODPALENIE $PZ1_{CE}$: źle wyszkolona ochrona $PZ2_{CE}$: brak nadzoru nad pracownikami ochrony 1(**N**) PZn_{CE}:		SPALONY BUDYNEK MZI=MRZ×PZ= =1×1=1 **MZI_{CE} = N**	10 mln. zł. **4(K)**	1×4=**4** **RYZYKO=K**
BŁ	1(**N**) ZAPRÓSZENIE OGNIA $PZ1_{BŁ}$: brak szkolenia p.poż. $PZ2_{BŁ}$: brak wyznaczonych stref dla palaczy 2(**S**) $PZn_{BŁ}$:...		SPALONY KOSZ NA ŚMIECI MZI=MRZ×PZ= =1×2=2 **$MZI_{BŁ}$=S**	200 zł. **1(N)**	2×1=**2** **RYZYKO=S**

Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska”, liczbowo „1”.

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 1. Szacowanie ryzyka dla zdarzenia o skutku „Pożar”

ANALIZA:

ARKUSZ nr 25 OPISU ZASOBU	
Typ zasobu: [infrastrukturalny, ~~teleinformatyczny, informacyjny, systemu ochrony~~]	
Identyfikator zasobu: [3/Moczarowa]	
Opis zasobu:	Czterokondygnacyjny budynek wykonany w technologii „Lipsk”
Umiejscowienie zasobu:	Opole, ul. Moczarowa 3
Właściciel zasobu:	Firma Płatnik Sp. z o.o., tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: nie dotyczy Integralności: nie dotyczy Dostępności: do 12 mln zł Rozliczalności: nie dotyczy
Inne dane w zależności od rodzaju zasobu:	Budynek wybudowany w 1979 roku

ARKUSZ nr 25.1 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: SW	
Zagrożenie:	Zjawisko atmosferyczne – burza z piorunami. Realizacja: piorun uderzający w dach obiektu [3/Moczarowa]
Scenariusz realizacji zagrożenia dla:	**Poufności:** NIE DOTYCZY **Integralności:** NIE DOTYCZY **Dostępności:** zależnie od stanu zabezpieczeń ppoż. oraz działania służb ochrony fizycznej obiektu i Straży Pożarnej może dojść: – tylko do uszkodzenia dachu budynku z powodu wznieconego przez piorun ognia oraz ograniczonych uszkodzeń infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty NISKIE); – uszkodzenia górnych pięter budynku z powodu wznieconego przez piorun ognia oraz ograniczonych uszkodzeń infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty ŚREDNIE); – wypalenia wszystkich pięter budynku z powodu wznieconego przez piorun ognia oraz zniszczenia

	infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty KRYTYCZNE); **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	[3/Moczarowa]/w skrajnym przypadku: całkowite spalenie budynku/xxx yyy *Zasoby powiązane: zasoby teleinformatyczne zlokalizowane w obiekcie (3/Moczarowa)*
Procesy, na które zagrożenie może mieć wpływ i szkody:	Wszystkie procesy biznesowe związane z zasobami teleinformatycznymi zlokalizowanymi w [3/Moczarowa]: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie, które są świadczone za pomocą zasobów teleinformatycznych zlokalizowanych w [3/Moczarowa]: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Wysoki: w przypadku strat KRYTYCZNYCH i braku infrastruktury zapasowej może doprowadzić do bankructwa firmy z powodu strat wywołanych zdarzeniem i utraty klientów z powodu przerwania świadczenia usług

Analogicznie należy wypełnić arkusze opisu zagrożenia nr 25.2 i 25.3 dla zagrożeń z klasy CE i BŁ.

Na podstawie analizy danych historycznych z Rejestru Ryzyka prowadzonego od 10 lat w firmie Płatnik sp. z o.o. (nie znaleziono zapisu incydentu „pożar wywołany uderzeniem pioruna") oraz uzyskanych z Komendy Głównej Straży Pożarnej w Opolu danych za ostatnie 10 lat nt. zdarzenia „pożar wywołany uderzeniem pioruna w zabudowie miejskiej" stwierdzono, że zdarzenie takie należy do zdarzeń rzadkich i przypisano mu ocenę opisową NISKIE (liczbowo 1).

Tab. 4. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu (3/Moczarowa)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
SW_D1(N)	PZ_{SWD} 2(S)	2(S)=1(N) × 2(S)	2(S)	2(S) × 2(S) = **4 (S)**

Opis zidentyfikowanych podatności:

W zakresie działania „sił wyższych” (SW_D) zidentyfikowano następujące podatności:

$PZ1_{SWD}$: brak instalacji odgromowej.

$PZ2_{SWD}$: niewłaściwie konserwowana instalacja odgromowa.

$PZ3_{SWD}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{SWD}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{SWD}$: niewłaściwie wdrożone DRP.

W zakresie celowej działalności człowieka (CE_D) zidentyfikowano następujące podatności:

$PZ1_{CED}$: źle wyszkolona ochrona fizyczna obiektów.

$PZ2_{CED}$: niewłaściwy nadzór nad pracownikami ochrony fizycznej obiektów.

$PZ3_{CED}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{CED}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{CED}$: niewłaściwie wdrożone DRP.

W zakresie błędów popełnianych przez człowieka ($BŁ_D$) zidentyfikowano następujące podatności:

$PZ1_{BŁD}$: brak szkolenia p.poż. dla pracowników firmy Płatnik sp. z o.o.

$PZ2_{BŁD}$: brak wyznaczonych stref dla palaczy.

$PZ3_{BŁD}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{CED}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{CED}$: niewłaściwie wdrożone DRP.

Komentarz: ponieważ to jest tylko przykład, zbiór podatności jest ograniczony. W praktyce, w ramach sesji burzy mózgów, identyfikowanie podatności i przygotowywanie ich opisów powinno być prowadzone tak długo, aż zabraknie pomysłów i/lub danych. Uwaga ta dotyczy także dwóch pozostałych przykładów. Z podanego przykładu widać (frazy zielone), że ta sama podatność może być istotna dla różnych sposobów realizacji zagrożenia o skutku „POŻAR”. Nasuwa to oczywisty wniosek, że zbiór takich podatności, na kolejnym etapie zarządzania ryzykiem (etap minimalizowania ryzyka), powinien być minimalizowany w pierwszej kolejności.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem „pożar” i (w tym przypadku) zagrożeniem typu SW_D. Na podstawie wyników wizji lokalnej przeprowadzonej przez eksperta stwierdzono,

że jest instalacja odgromowa, ale jest źle konserwowana, czyli całkowity poziom podatności w tym przypadku oceniono jako ŚREDNI (liczbowo 2). Szczegóły – patrz tabela 5.

Tab. 5. Interpretacja ocen opisowych dla podatności[7] związanych ze zdarzeniem „pożar" i zagrożenia typu SW_D

OCENA	INTERPRETACJA
K	~(jest instalacja odgromowa) ∧ ~(właściwa konserwacja instalacji odgromowej)
W	–
S	~(jest instalacja odgromowa) ∧ (właściwa konserwacja instalacji odgromowej) ∨ (jest instalacja odgromowa) ∧ ~(właściwa konserwacja instalacji odgromowej)
N	(jest instalacja odgromowa) ∧ (właściwa konserwacja instalacji odgromowej)

Uwaga: symbole ∧, ∨ oraz ~ to funktory zdaniotwórcze odpowiednio „i", „lub" oraz „nieprawda, że". Uwaga ta dotyczy także pozostałych dwóch przykładów.

Po zasięgnięciu opinii eksperta z dziedziny ochrony ppoż. stwierdzono, że pomimo złej konserwacji instalacji odgromowej, ze względu na niewielką odległość obiektu od remizy Straży Pożarnej, szkody w najgorszym przypadku powinny się ograniczyć do spalenia górnych pięter budynku i ograniczonych uszkodzeń infrastruktury teleinformatycznej. Szacunkowe straty wyceniono na ok. 95 tys. zł. Czyli poziom strat oceniono jako ŚREDNI (liczbowo 2).

Oszacowania są zebrane w tabeli 4. Z przyjętej metody szacowania ryzyka (patrz [3]) wynika, że ryzyko zajścia zdarzenia:

ZD_25: Pożar w budynku firmy Płatnik Sp. z o.o. przy ul. Moczarowej 3 w Opolu

na skutek realizacji zagrożenia typu „siła wyższa" jest na poziomie ŚREDNI.

Tabelę 4 należy uzupełnić o oszacowania utraty dostępności obiektu (zasobu infrastrukturalnego) 3/Moczarowa na skutek pożaru wywołanego celową działalnością człowieka (CE_D) oraz błędami popełnionymi przez człowieka ($BŁ_D$). Elementy takiej analizy są zamieszczone na rys. 1.

[7] W tej tabeli liczbę podatności ograniczono do dwóch. W praktyce ich liczba będzie zależna od wyników identyfikacji, a sposób ich złożenia, w celu uzyskania interpretacji ocen, będzie zależał od wiedzy i decyzji analityka ryzyka lub wspierającego go eksperta dziedzinowego. Uwaga ta dotyczy także pozostałych przykładów.

3. **Szacowania ryzyka IT – przypadek 2** (bez SW i CE)

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną
o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik sp. z o.o., jest zdarzenie:

ZD_35: Błąd w oprogramowaniu firmy Płatnik sp. z o.o. uniemożliwiający prawidłową realizację płatności Klienta

Stwierdzono przy tym, że występujący błąd nie może być wynikiem sabotażu (czyli realizacji zagrożenia z klasy CE), a klasa SW z oczywistych względów nie jest brana pod uwagę.

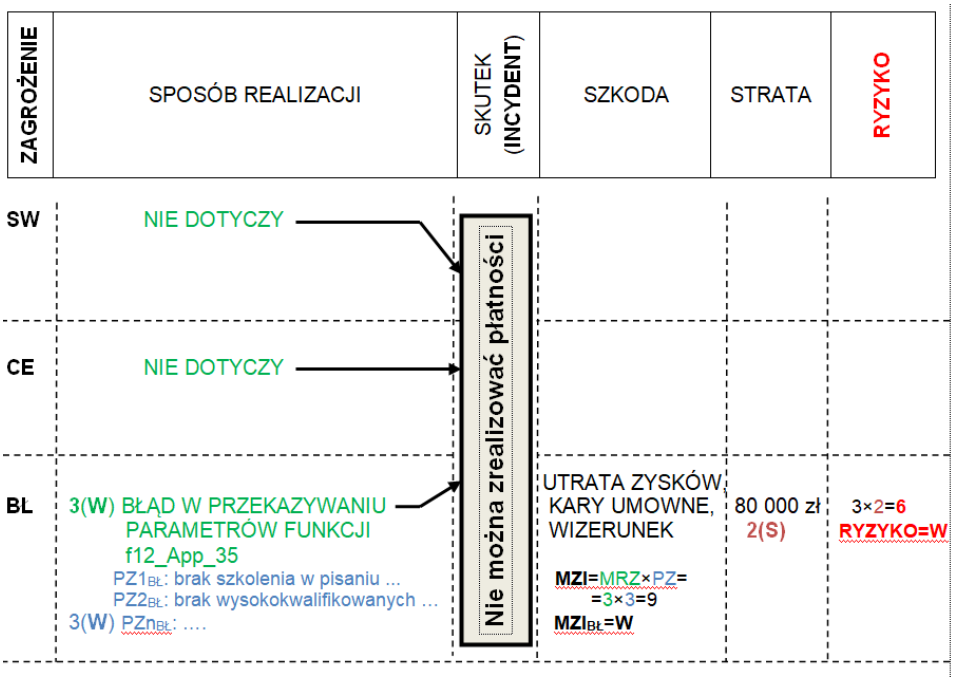
Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 6.

Tab. 6. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok

Dalej jest przedstawiona szczegółowa analiza dla zagrożenia klasy **BŁ** realizującego się jako „Błąd w przekazywaniu parametrów funkcji f12_App_35".

Schemat wykonanej analizy przedstawiono na rysunku 2.



Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska”, liczbowo „1”.

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 2. Szacowanie ryzyka dla zdarzenia o skutku „Nie można zrealizować płatności”

ANALIZA:

ARKUSZ nr 35 OPISU ZASOBU	
Typ zasobu: [~~infrastrukturalny, teleinformatyczny~~, informacyjny, ~~systemu ochrony~~]	
Identyfikator zasobu: [App_35/Platnik]	
Opis zasobu:	Moduł realizacji płatności Klienta wykonany w Pythonie
Umiejscowienie zasobu:	Chmura AWS
Właściciel zasobu:	Firma Płatnik Sp. z o.o., tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: nie dotyczy Integralności: nie dotyczy Dostępności: do 100 tys. zł Rozliczalności: nie dotyczy

Inne dane w zależności od rodzaju zasobu:	Wykonawcą błędnego modułu jest ZP_3

ARKUSZ nr 35.3 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: BŁ	
Zagrożenie:	Błąd kodowania popełniony przez zespół programistyczny ZP_3.
Scenariusz realizacji zagrożenia dla:	**Poufności:** NIE DOTYCZY **Integralności:** NIE DOTYCZY **Dostępności:** Po zainstalowaniu w środowisku produkcyjnym nowej wersji modułu App_35/Platnik, u kilku klientów realizujących operacje płatnicze został zasygnalizowany błąd (Error 35) sugerujący nieprawidłowe działanie funkcji f12_App_35. Skutkiem tego błędu było przerwanie realizacji płatności. Oprócz komunikatu (Error 35), na ekranie klienta nie zostały wyświetlone żadne inne informacje, a program zawiesił swoje działanie. **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	Wszystkie funkcje wywoływane z modułu App_35/Płatnik
Procesy, na które zagrożenie może mieć wpływ i szkody:	Wszystkie biznesowe procesy płatnicze: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie usługi płatnicze: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Wysoki: część klientów nie może realizować płatności, co rzutuje na wizerunek firmy Płatnik Sp. z o.o. jako wiarygodnego dostawcy usług płatniczych. Tracone są zyski z niezakończonych transakcji, niektórym sklepom internetowym muszą być wypłacone kary umowne.

Oprogramowanie płatnicze jest uaktualniane średnio co trzy miesiące przez programistów zatrudnionych w firmie Płatnik. Na podstawie analizy danych historycznych z Rejestru Ryzyka prowadzonego od 10 lat w firmie Płatnik stwierdzono, że zdarzenie typu „błąd w oprogramowaniu, którego skutkiem jest

brak możliwości zrealizowania operacji płatniczej" występuje średnio raz w ciągu roku (tj. co czwartą aktualizację). Powiadamiany o incydentach Zarząd firmy Płatnik uznał, że w związku z ostrą konkurencją na rynku usług płatniczych częstość występowania błędu tego typu jest zbyt duża i należy dążyć do jej zmniejszenia. Aktualną częstość występowania tego błędu oceniono w związku z tym jako WYSOKĄ (liczbowo 3).

Tab. 7. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu (App_35/Platnik)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
BŁ$_D$ 3(W)	PZ$_{BŁD}$ 3(W)	9(W) = 3(W) × 3(W)	2(S)	3(W) × 2(S) = **6(W)**

Opis zidentyfikowanych podatności:

PZ1$_{BŁD}$: brak szkolenia z pisania bezpiecznego kodu dla programistów z firmy Płatnik sp. z o.o.

PZ2$_{BŁD}$: brak w zespole ZP_3 programistów o wysokich kwalifikacjach.

PZ3$_{BŁD}$: niewykonywanie testów regresyjnych zaktualizowanego oprogramowania w środowisku zapasowym przed zainstalowaniem w środowisku produkcyjnym.

PZ4$_{BŁD}$: niewłaściwy nadzór nad procesem testowania.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem ZD_35 i (w tym przypadku) zagrożeniem typu BŁ$_D$. Na podstawie wywiadów z programistami z zespołu ZP_3 stwierdzono, że wszyscy są programistami młodszymi i nie przeszli żadnego szkolenia z pisania bezpiecznego kodu. Całkowity poziom podatności w tym przypadku oceniono jako WYSOKI (liczbowo 3). Szczegóły – patrz tabela 8.

Tab. 8. Interpretacja ocen opisowych dla podatności związanych ze zdarzeniem ZD_35 i zagrożenia typu BŁ

OCENA	**INTERPRETACJA**
K	–
W	~(jest starszy programista w zespole) ∧ ~(są szkolenia z pisania bezpiecznego kodu)
S	~(jest starszy programista w zespole) ∧ (są szkolenia z pisania bezpiecznego kodu) ∨ (jest starszy programista w zespole) ∧ ~(są szkolenia z pisania bezpiecznego kodu)
N	(jest starszy programista w zespole) ∧ (są szkolenia z pisania bezpiecznego kodu)

Po zasięgnięciu opinii dyrektora działu ds. kluczowych klientów stwierdzono, że błąd tego typu ujawnia się tylko w przypadku szczególnych kombinacji wprowadzanych przez klientów znaków, co oznacza że kluczowi klienci albo zostali dotknięci tym błędem tylko raz w ciągu 10 lat (jak wynika z Rejestru Ryzyka) lub wcale. W związku z tym uznano, że szkody w najgorszym przypadku powinny się ograniczyć do nieznacznych strat wizerunkowych oraz sporadycznie wypłaconej kary umownej. Szacunkowe straty wyceniono na ok. 80 tys. zł, czyli poziom strat oceniono jako ŚREDNI (liczbowo 2).

Oszacowania są zebrane w tabeli 7. Z przyjętej metody szacowania ryzyka (patrz [3]) wynika, że ryzyko zajścia zdarzenia:

ZD_35: Błąd w oprogramowaniu firmy Płatnik sp. z o.o., uniemożliwiający prawidłową realizację płatności Klienta

na skutek realizacji zagrożenia typu „błąd ludzki" jest na poziomie WYSOKI.

4. Szacowania ryzyka IT – przypadek 3 (bez SW i BŁ)

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik sp. z o.o., jest zdarzenie:

ZD_42: Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik sp. z o.o.

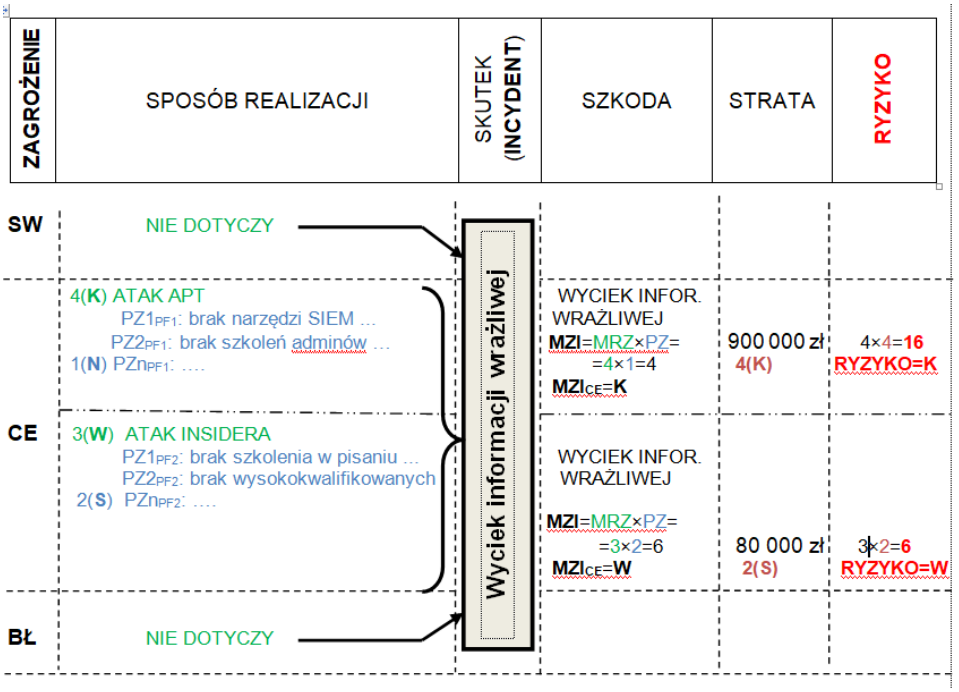
Stwierdzono, że istnieją dwa realne scenariusze wydarzeń (oba z klasy **CE**):

1) wrogi **podmiot wewnętrzny** (ang. *insider*) wyprowadził informacje nt. umów podpisanych z klientami firmy Płatnik sp. z o.o.;
2) wrogi **podmiot zewnętrzny** skutecznie zrealizował atak typu APT i w ciągu 6 miesięcy wyprowadził dane nt. wszystkich umów firmy Płatnik sp. z o.o.

Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 9.

Tab. 9. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok



Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska", liczbowo „1".

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 3. Szacowanie ryzyka dla zdarzenia o skutku „Wyciek informacji wrażliwej"

Dalej jest przedstawiona szczegółowa analiza dla zagrożenia klasy **CE** (dwa warianty) realizującego się jako: „Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik sp. z o.o.". Schemat wykonanej analizy przedstawiono na rysunku 3.

ANALIZA:

ARKUSZ nr 42 OPISU ZASOBU	
Typ zasobu: [~~infrastrukturalny, teleinformatyczny~~, informacyjny, ~~systemu ochrony~~]	
Identyfikator zasobu: [Katalog_UMOWY]	
Opis zasobu:	W katalogu UMOWY są przechowywane w plikach .docx i .pdf umowy zawarte z dostawcami usług i usługobiorcami firmy Płatnik Sp. z o.o.
Umiejscowienie zasobu:	Chmura AWS (kopia), dysk w stacji roboczej ST_22 w siedzibie firmy Płatnik Sp. z o.o.
Właściciel zasobu:	Firma Płatnik sp. z o.o. , tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: 900 000 zł Integralności: nie dotyczy Dostępności: nie dotyczy Rozliczalności: nie dotyczy
Inne dane w zależności od rodzaju zasobu:	Stacja robocza ST_22 należy do Działu Księgowości

ARKUSZ nr 42.1 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: CE	
Zagrożenie:	Wrogi podmiot wewnętrzny realizujący atak fizyczny i wrogi podmiot zewnętrzny realizujący atak zdalny.
Scenariusz realizacji zagrożenia dla:	**Poufności:** 1) Wrogi podmiot zewnętrzny (CE_{PF1}): W wyniku wykrytego i zablokowanego dopiero po 172 dniach ataku APT zostały wyprowadzone dane wszystkich umów zarówno zarchiwizowanych, jak i zawartych w czasie trwania ataku. 2) Wrogi podmiot wewnętrzny (*insider*; CE_{PF2}): Po zmianie zarządu firmy i licznych zwolnieniach z pracy, znacząco pogorszyły się stosunki pomiędzy personelem i kierownictwem. Spowodowało to zwiększoną podatność pracowników na przekupstwo ze strony konkurencji. Jeden z przekupionych pracowników księgowości mający legalny dostęp do zasobu teleinformatycznego ST_22, zanim odebrano mu dostęp do obiektów i systemów firmy Płatnik, korzystając z aparatu fotograficznego (zdjęcia ekranu monitora komputera), wyprowadził dane o 10 umowach zawartych z usługobiorcami firmy Płatnik w ciągu ostatnich trzech miesięcy. **Integralności:** NIE DOTYCZY **Dostępności:** NIE DOTYCZY **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	Brak
Procesy, na które zagrożenie może mieć wpływ i szkody:	Procesy związane z organizacją przetargów: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie zamawiane usługi: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Średni: rzutuje na wizerunek firmy Płatnik Sp. z o.o. jako wiarygodnego partnera biznesowego.

Tab. 10. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu POUFNOŚĆ dla zasobu (Chmura AWS/ST_22)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_P$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
CE_{PF1}: 4(K) CE_{PF2}: 3(W)	PZ_{PF1} 1(N) PZ_{PF2} 2(S)	4(K) =4(K) × 1(N) 6(W) = 3(W) × 2(S)	4(K) 2(S)	4(K) × 4(K) = **16(K)** 3(W) × 2(S) = **6(W)**

Opis zidentyfikowanych podatności:

$PZ1_{PF1}$: brak narzędzi typu SIEM.

$PZ1_{PF2}$: brak mechanizmów zapewniania lojalności pracowników.

$PZ2_{PF1}$: administratorzy techniczni sieci i systemów nie zostali przeszkoleni w zakresie rozpoznawania symptomów ataków zdalnych.

$PZ2_{PF2}$: brak procedur bezpieczeństwa pracy z informacjami wrażliwymi.

$PZ3_{PF1}$: dzienniki zdarzeń systemów i urządzeń nie są przeglądane w celu znalezienia anomalii świadczących o ataku.

$PZ3_{PF2}$: brak procedur nadzoru nad działaniami pracowników ze strony personelu Departamentu Bezpieczeństwa.

$PZ4_{PF1}$: brak procedur pozyskiwania informacji o najnowszych sposobach realizacji ataków i ich symptomach.

$PZ4_{PF2}$: brak narzędzi z zakresu ochrony technicznej (kamer, rejestratorów WE/WY itp.) umożliwiających nadzór nad działaniami pracowników.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem ZD_42 i (w tym przypadku) zagrożeniem typu CE_{PF1} i CE_{PF2}. Na podstawie wyników wizji lokalnej przeprowadzonej przez eksperta oraz podstawie wywiadów z personelem Departamentu Bezpieczeństwa i Księgowości stwierdzono że:

- W zakresie CE_{PF1} – admini techniczni są regularnie kierowani na szkolenia z zakresu rozpoznawania symptomów ataków zdalnych oraz wykorzystują w swojej pracy narzędzia SIEM, czyli poziom podatności oceniono jako NISKI (liczbowo 1).
- W zakresie CE_{PF2} – jest co prawda nadzór ze strony Departamentu Bezpieczeństwa nad działaniami pracowników, ale w firmie nie ma wdrożonych żadnych mechanizmów zapewniania lojalności, czyli poziom podatności oceniono jako ŚREDNI (liczbowo 2).Szczegóły – patrz tabela 11.

Tab. 11. Interpretacja ocen opisowych dla podatności związanych ze zdarzeniem ZD_42 i zagrożenia typu CE

OCENA	INTERPRETACJA
K /CE_{PF1}	~(są używane SIEM) ∧ ~(admini są przeszkoleni)
W/CE_{PF1}	–
S/CE_{PF1}	~(są używane SIEM) ∧ (admini są przeszkoleni) ∨ (są używane SIEM) ∧ ~(admini są przeszkoleni)
N/CE_{PF1}	(są używane SIEM) ∧ (admini są przeszkoleni)
K/CE_{PF2}	–
W/CE_{PF2}	~(jest nadzór) ∧ ~(są mechanizmy zapewniania lojalności)
S/CE_{PF2}	~(jest nadzór) ∧ (są mechanizmy zapewniania lojalności)∨ (jest nadzór) ∧ ~(są mechanizmy zapewniania lojalności)
N/CE_{PF2}	(jest nadzór) ∧ (są mechanizmy zapewniania lojalności)

Dla CE_{PF1}: Po sprawdzeniu Rejestru Ryzyka stwierdzono, że w minionych dziesięciu latach było 5 przypadków ataków typu APT o średnim czasie wykrycia 20 dni (przy średniej światowej 180 dni). Biorąc pod uwagę wzmożoną działalność grup APT oraz fakt, że Płatnik jest instytucją finansową (czyli atrakcyjnym celem dla przestępczych podmiotów zewnętrznych), oceniono możliwość zaistnienia w najbliższym czasie ataku APT jako KRYTYCZNĄ (liczbowo 4), a przypuszczalne straty związane z karami umownymi wyceniono na ok. 900 000 zł, czyli także jako KRYTYCZNE (liczbowo 4).

Dla CE_{PF2}: Po sprawdzeniu Rejestru Ryzyka stwierdzono, że w minionych dziesięciu latach nie było przypadków nielojalnych działań pracowniczych. Możliwość przeprowadzenia szkodliwych działań przez *insidera* z perspektywy historycznej oceniono zatem jako niską. Ale uwzględniając aktualne trendy w działaniu grup APT (wzmożone pozyskiwanie *insiderów*) oraz występujące po raz pierwszy od dziesięciu lat poważne konflikty na linii Zarząd-pracownicy, zdecydowano, że możliwość przeprowadzenia szkodliwych działań przez wrogi podmiot wewnętrzny należy ocenić jako WYSOKĄ (liczbowo 3). Biorąc pod uwagę to, że poszczególni pracownicy mają dostęp do zasobów informacyjnych, przyznawany na zasadzie „wiedzy koniecznej" i „minimalnego środowiska pracy" (czyli w praktyce mogą ujawnić tylko część umów) oraz wysokość kar umownych związanych z ujawnieniem informacji wrażliwych, oszacowano możliwe straty na ok. 80 tys. zł, czyli jako ŚREDNIE (liczbowo 2).

Oszacowania są zebrane w tabeli 10. Z przyjętej metody szacowania ryzyka (patrz [3])[8] wynika, że ryzyko zajścia zdarzenia:

ZD_42: Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik Sp. z o.o.

na skutek realizacji zagrożenia typu „Działanie celowe" jest na poziomie KRYTYCZNY.

4. Podsumowanie

W artykule przedstawiono trzy przykłady szacowania ryzyka IT. Przykłady te, dla których podstawy formalne są zawarte w pracach [1] i [3], uwzględniają następujące założenia:

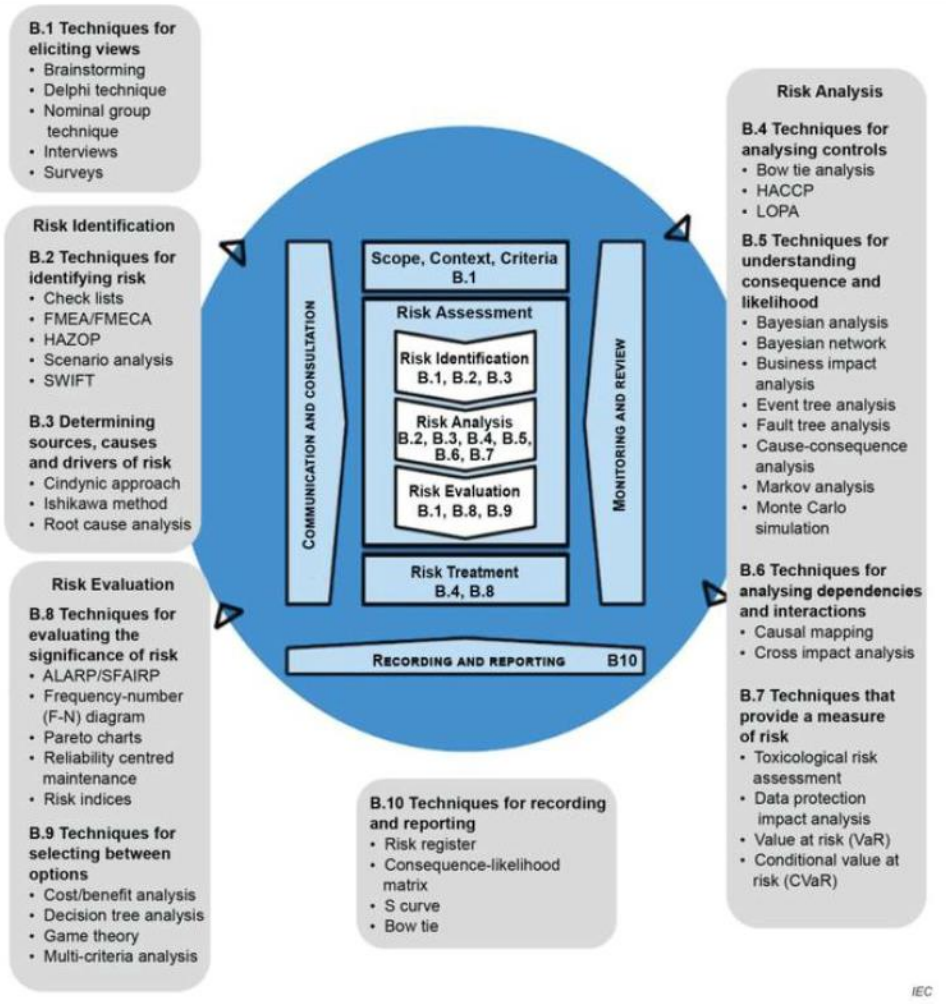
1. Zbiór zagrożeń jest trójelementowy (SW, CE, BŁ).
2. Metody szacowania to:
   - metoda autorska (patrz [1], [3]), opisowa, wykorzystująca oceny opisowe ze zbioru {**N**iskie, **Ś**rednie, **W**ysokie, **K**rytyczne} oraz
   - metoda według ISO/IEC 27005 [6] wykorzystująca oceny liczbowe ze zbioru {**1**, **2**, **3**, **4**}.
3. Dostępne są dane historyczne, np. z Rejestru Ryzyka prowadzonego przez podmiot, dla którego jest prowadzona analiza ryzyka oraz dane z wywiadów z ekspertami.

Celem artykułu było pokazanie możliwości praktycznego wyliczenia wartości ryzyka. Warto zauważyć, że konsekwentnie rozróżnianie zagrożenia i sposobu jego realizacji[9], co jest pokazane na rys. 1-3, uwidacznia w zakresie minimalizacji ryzyka możliwości działania proaktywnego, które to możliwości zwykle są niedostrzegane przy „widzeniu" tylko zagrożenia i jego skutku (np. na rys. 1 – pożaru).

Dla Czytelnika, który jest zainteresowany szerszym spektrum technik stosowanych przy ocenie ryzyka (głównie jakościowych), warta polecenia jest norma [7], która zawiera specyfikację i opis 40 technik szacowania ryzyka przyporządkowanych do procesów zarządzania ryzykiem według normy [5] (patrz rys. 4).

[8] $\max\{\text{RYZYKO}(CE_{PF1}), \text{RYZYKO}(CE_{PF2})\} = \max\{K, W\} = \mathbf{K}$

[9] Czyli także uwidocznienie podatności, które mogą być wykorzystane przy konkretnej realizacji zagrożenia i które mogą być w ramach przeciwdziałania tej konkretnej realizacji minimalizowane.



Rys. 4. Zastosowanie technik szacowania ryzyka w procesie zarządzania ryzykiem według normy ISO 31000 (za [7])

Literatura

[1] LIDERMAN K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa, 2017.

[2] LIDERMAN K., *Risk of undesired changes to significant information quality criteria*, Teleinformatics Review, Nr 3-4(47), WAT, Warszawa 2019, pp. 31-55.

[3] LIDERMAN K., *Analiza ryzyka na potrzeby bezpieczeństwa informacyjnego według zaleceń normy PN-ISO/IEC 27005*. Przegląd Teleinformatyczny, Nr 8(26) 1-4. WAT, Warszawa 2022, s. 19-34.

[4] COBIT® 5, *Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*, An ISACA® Framework, wersja językowa polska.

[5] PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN 2012.

[6] PN-ISO/IEC 27005:2014, *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*, PKN 2014

[7] PN-EN IEC 31010:2020-01, *Zarządzanie ryzykiem – Techniki oceny ryzyka*, wersja językowa angielska.

IT risk evaluation – case study

ABSTRACT: The paper presents, through three examples, an IT risk evaluation method. IT risk is associated with the realization of threats that cause damage to teleinformatics systems and processed information resources. The quality risk evaluation method, demonstrated through these examples, involves four descriptive scores translated into numerical values in accordance with the PN-ISO/IEC 27005:2014-01 recommendation.

KEYWORDS: information security, threat realization, IT risk evaluation

Praca wpłynęła do redakcji: 29.11.2022 r.

PRZEGLĄD TELEINFORMATYCZNY
NR 00, 2023

Bezpieczna i wydajna wymiana danych w sieciach Internetu Rzeczy – przegląd technologii

Sebastian ŁESKA

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
sebastian.leska@wat.edu.pl

STRESZCZENIE: Urządzeniom IoT często towarzyszą liczne ograniczenia sprzętowe, takie jak ograniczona moc obliczeniowa, ograniczone zasoby pamięciowe oraz niska przepustowość sieci. Wszystkie te składową mają znaczący wpływ na trudności w zapewnieniu bezpieczeństwa sieciom IoT. Z tego powodu powstały różne rozwiązania przeznaczone specjalnie dla urządzeń IoT, mające na celu podniesienie poziomu bezpieczeństwa takich urządzeń. W artykule dokonano przeglądu najpopularniejszych rozwiązań wykorzystywanych w sieciach IoT, które minimalizują problemy spowodowane licznymi ograniczeniami.

SŁOWA KLUCZOWE: IoT, bezpieczeństwo sieci IoT, dystrybucja kluczy symetrycznych, lekkie protokoły wymiany danych, interfejsy komunikacyjne IoT

Wprowadzenie

Początek XXI wieku to czas, w którym wiele badań i pracy przeznaczonych zostało na rozwój i wzrost liczby zastosowań technologii Internetu Rzeczy (ang. *Internet of Things* – IoT). Dzięki dynamicznemu rozwojowi technologii IoT możliwe jest coraz szersze wykorzystywanie oferowanych przez nie usług oraz wdrażanie nowych rozwiązań w różnych obszarach życia i pracy. Masowa produkcja urządzeń IoT wymaga jednak, aby koszt takich urządzeń był niewielki, a to oznacza, że producenci narzucają duże ograniczenia związane m.in. z mocą obliczeniową, zasobami pamięciowymi i prędkością transmisji danych. Szybki rozwój oraz tania produkcja urządzeń, a co za tym idzie, niewystarczająca dbałość o bezpieczeństwo, są przyczyną nieustannie rosnącej liczby zagrożeń oraz punktów ataku na sieci IoT ze względu na niewystarczające zabezpieczenia

urządzeń. W tym celu konieczne jest opracowanie rozwiązania zapewniającego bezpieczną wymianę danych oraz budowę zaufanego środowiska IoT.

1. Budowa zaufanego środowiska dla sieci IoT

Jednym z najistotniejszych problemów związanych z projektowaniem sieci IoT jest zapewnienie zaufania pomiędzy węzłami sieci. Każdy z węzłów powinien mieć pewność dotyczącą tożsamości i wiarygodności pozostałych stron biorących udział w wymianie danych. Zaufanie pomiędzy węzłami sieci można osiągnąć poprzez implementację mechanizmu uwierzytelniania.

1.1. Kryptografia asymetryczna

W tradycyjnych sieciach wykorzystujących protokół IP w celu zweryfikowania innego węzła stosuje się certyfikaty i podpisy cyfrowe. Jest to najbezpieczniejszy sposób uwierzytelniania, jednakże jego zastosowanie nie zawsze jest możliwe w sieciach IoT.

Do stosowania certyfikatów konieczna jest obecność zaufanej trzeciej strony biorącej udział w komunikacji pomiędzy dwoma węzłami, której rolę pełni Urząd Certyfikujący (ang. *Certificate Authority* – CA). Zadaniem CA jest weryfikacja danych zawartych w wysłanym żądaniu CSR (ang. *Certificate Signing Request*), do których zalicza się klucz publiczny oraz informacje o stronie aplikującej (np. domena, e-mail). W przypadku stwierdzenia poprawności otrzymanych danych, CA potwierdza tożsamość aplikanta poprzez wystawienie certyfikatu (podpisanie cyfrowe żądania CSR) oraz odesłanie go z powrotem. Certyfikat taki może zostać wysłany do dowolnego podmiotu w sieci, a jego obecność świadczy o wiarygodności nadawcy, zapewniając odbiorcę, że jego rozmówca jest tym, za kogo się podaje. Rozwiązanie to jest często deklasowane w sieciach IoT z powodu ich częstej niezależności od sieci Internet, a tym samym braku dostępu do istniejących CA.

Certyfikacja i podpisy cyfrowe są elementem kryptografii asymetrycznej, co oznacza, że konieczne jest stosowanie przez węzły sieci kluczy prywatnych i publicznych. Szyfrowanie asymetryczne standardowo wykorzystuje klucze o długości 2048 bitów, natomiast szyfrowanie symetryczne zazwyczaj stosuje klucze o długości 256 bitów. Oznacza to, że do obsługi kryptografii asymetrycznej konieczne jest dysponowanie większymi zasobami pamięciowymi oraz większą przepustowością sieci. W przypadku węzłów IoT często może brakować miejsca w pamięci na przechowywanie wielu takich kluczy, co uniemożliwiłoby im komunikację z częścią węzłów sieci. Dodatkowo w sieciach IoT często stosuje się interfejsy sieciowe zaprojektowane specjalnie dla urządzeń IoT, umożliwiające

bezprzewodową transmisję danych na duże odległości, jednakże z niewielką przepustowością, co oznacza, że konieczne jest ograniczenie liczby transmitowanych bajtów do minimum w celu zapewnienia wydajnej komunikacji.

1.2. Uwierzytelnianie z wykorzystaniem hasła

Jedną z najprostszych metod uwierzytelniania jest implementacja obsługi hasła. Użytkownik pragnący uzyskać dostęp do określonych zasobów bądź usług zobowiązany jest podać ustalone wcześniej hasło, które będzie świadczyło o jego wiarygodności. Hasło to wprowadza się jako ciąg znaków ASCII, który następnie poddawany jest obróbce funkcji skrótu i wysyłany do serwera w celu porównania otrzymanego skrótu z zapisanym w lokalnych zasobach skrótem. W przypadku gdy serwer stwierdzi, że hasło jest prawidłowe, wygenerowany zostanie dla klienta unikatowy token, który może być wykorzystywany do uwierzytelniania i autoryzacji bez konieczności ciągłego podawania hasła.

Metoda z wykorzystaniem hasła jest prosta w implementacji i szybka w obsłudze, a do tego nie obciąża zasobów pamięciowych ani łącza danych. Wadą jest fakt, że opcja ta nie jest tak bezpieczna, jak wykorzystanie kryptografii asymetrycznej. W tym przypadku konieczne jest stosowanie bezpiecznego hasła, które będzie wymieniane co pewien czas. Słabe hasło szybko mogłoby zostać złamane, dając nieautoryzowany dostęp do zasobów niepożądanym podmiotom. Dodatkowo stosowanie hasła wymaga, aby urządzenia były obsługiwane przez ludzi, którzy te hasła by wprowadzali, a w sieciach przemysłowych IoT konieczna jest pełna automatyzacja niewymagająca interwencji człowieka.

1.3. Uwierzytelnianie z wykorzystaniem kontekstu

Jedną z mniej znanych metod uwierzytelniania jest metoda wykorzystująca kontekst urządzenia. Rozwiązanie to polega na użyciu unikatowych cech urządzenia w procesie potwierdzania swojej tożsamości. Kontekst może składać się z wielu cech urządzenia, a każdą cechą może być charakterystyczna informacja, począwszy od uruchomionego systemu, numerów seryjnych, a skończywszy na pomiarach napięć na płytce. Zestaw takich cech tworzy kontekst, który jest w stanie jednoznacznie odróżnić jedno urządzenie od drugiego, tym samym umożliwiając jego uwierzytelnienie.

Rozwiązanie to jest proste w implementacji i umożliwia łatwą automatyzację pracy sieci, gdyż nie jest konieczna ingerencja człowieka do uwierzytelniania węzłów sieci. Metoda ta ma jednak jeden mankament, a mianowicie w przypadku dokonania niewielkiej zmiany na urządzeniu nie będzie możliwe dalsze uwierzytelnianie tego urządzenia w sieci i w takiej sytuacji konieczne będzie podjęcie stosownych działań. Z tego powodu niezwykle ważne

jest, aby dobrać taki zestaw cech, dzięki któremu możliwe będzie prawidłowe uwierzytelnienie urządzenia z równoczesnym minimalizowaniem ryzyka zmiany tych cech w czasie eksploatacji urządzenia.

2. Zapewnienie bezpiecznej transmisji danych z zachowaniem skalowalności sieci

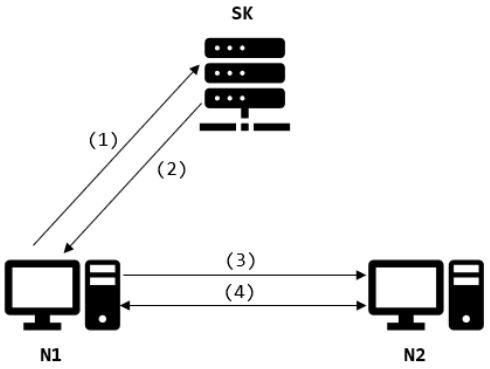
Ze względu na liczne ograniczenia urządzeń IoT, często niemożliwe jest stosowanie kryptografii asymetrycznej do zabezpieczenia transmisji danych. Oznacza to, że konieczne jest stosowanie kryptografii symetrycznej. Niesie to ze sobą jednak pewien problem, którym jest dystrybucja klucza symetrycznego. W przypadku nawiązania komunikacji pomiędzy dwoma węzłami, sprawa jest prosta, ponieważ można wykorzystać jeden z protokołów ustalania klucza wspólnego, do których należy protokół Diffiego-Hellmana bądź ECDH (ang. *Eliptic Curve Diffie-Hellman*). Sprawa jednak się komplikuje w momencie w którym konieczne jest zapewnienie skalowalności sieci, w której grupa węzłów będzie mogła stosować jeden klucz do zabezpieczenia transmisji danych. W takiej sytuacji konieczne jest wdrożenie protokołu dystrybucji klucza.

2.1. Key Distribution Center

Jednym z pierwszych rozwiązań umożliwiających dystrybucję klucza do wielu węzłów jest protokół Needham-Schroeder [1] opracowany w 1978 r. Rozwiązanie zakłada istnienie w sieci węzła pełniącego funkcję Centrum Dystrybucji Kluczy (ang. *Key Distributrion Center* – KDC) i odpowiedzialnego za generowanie i dystrybucję kluczy symetrycznych (sesji) na żądanie. Zgodnie z tą koncepcją, klucze są generowane w węźle centralnym, a dopiero potem wysyłane do poszczególnych węzłów. W celu umożliwienia takiego rozwiązania konieczne jest wcześniejsze ustalenie przez każdy dołączający do sieci węzeł klucza głównego (np. z wykorzystaniem protokołu Diffiego-Hellmana) z węzłem centralnym. Klucz ten wykorzystywany jest do zabezpieczenia dalszej transmisji danych pomiędzy tymi dwoma węzłami, w tym do zaszyfrowania transmitowanego klucza sesji. Ważne jest, aby ze względów kryptoanalitycznych klucz główny miał większą długość niż klucz sesji.

Po dołączeniu do sieci każdego klienta (Ni), węzeł centralny pełni funkcję serwera kluczy (SK) i przechowuje w swoich zasobach klucze główne wszystkich węzłów sieci. Po ustaleniu kluczy głównych dystrybucja klucza sesji odbywa się w czterech krokach (rys. 1):

1) **E(K_{N1}, R) –** wysłanie przez węzeł N1 do węzła SK żądania (R) wygenerowania klucza symetrycznego do komunikacji z węzłem N2, zaszyfrowanego kluczem głównym węzła N1.
2) **E(K_{N1}, E(K_{N2}, K_S)+K_S) –** wysłanie przez SK odpowiedzi składającej się z paczki dla węzła N2, zaszyfrowanej jego kluczem głównym oraz zawierającej klucz sesji K_S, a także paczki dla węzła N1, dołączonej na koniec paczki węzła N2, całość zaszyfrowana kluczem głównym węzła N1.
3) **E(K_{N2}, K_S) –** przesłanie do węzła N2 paczki przygotowanej przez SK, otrzymanej w wyniku odszyfrowania odpowiedzi serwera przez węzeł N1.
4) Testowanie przez węzły N1 i N2 nowo otrzymanego klucza Ks.



Rys. 1. Schemat dystrybucji klucza metodą KDC

2.2. Key Translation Center

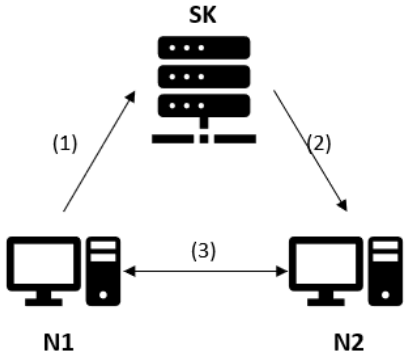
Stosowanie KDC daje gwarancję dotyczącą wiarygodności wygenerowanych kluczy dzięki pewności co do zastosowanego źródła entropii oraz wykorzystanych procedur. Rozwiązanie to jednak może być czasochłonne ze względu na złożoność obliczeniową funkcji generowania kluczy. Oznacza to, że przy wielu równoczesnych żądaniach wygenerowania klucza węzeł centralny nie będzie w stanie odpowiedzieć każdemu klientowi na czas. Z tego powodu powstała nowa metoda dystrybucji kluczy, polegająca na zastosowaniu Centrum Tłumaczenia Kluczy (ang. *Key Translation Center* – KTC) [2].

Rozwiązanie to, podobnie jak KDC, wymaga ustalenia z każdym klientem klucza głównego, jednakże w tym przypadku węzeł centralny nie generuje samodzielnie kluczy sesji, a jedynie odpowiada za ich odszyfrowanie kluczem głównym jednego węzła i zaszyfrowanie kluczem głównym drugiego węzła. Klucze sesji generowane są przez klienta i wysyłane do KTC w celu ich przetłumaczenia dla innego węzła końcowego. Podejście takie jest zdecydowanie bardziej oszczędne czasowo i zużywa mniej zasobów sprzętowych węzła

centralnego dzięki brakowi konieczności wykonywania operacji generowania klucza, jednakże jest mniej bezpieczne z powodu braku pewności co do wykorzystanego źródła entropii i procedur generowania klucza.

Dystrybucja klucza wykorzystująca rozwiązanie KTC przeprowadzana jest w 3 krokach, które opisane zostały na rysunku 2:

1) **$E(K_{N1}, Ks)$ –** wysłanie przez węzeł N1 wygenerowanego klucza Ks z żądaniem przetłumaczenia go dla klucza N2; żądanie zaszyfrowane kluczem głównym węzła N1.
2) **$E(K_{N2}, K_S)$ –** przesłanie do węzła N2 klucza Ks zaszyfrowanego kluczem głównym N2.
3) Testowanie przez węzły N1 i N2 klucza Ks.



Rys. 2. Schemat dystrybucji klucza metodą KTC

3. Zapewnienie wydajnej transmisji danych

Jedną z cech charakterystycznych urządzeń sieci IoT jest wymaganie dotyczące niskiego zużycia energii. Urządzenia IoT rzadko wykorzystują interfejsy umożliwiające komunikację w sieci Internet. W zdecydowanej większości wymiana danych odbywa się z wykorzystaniem Bluetooth, a coraz częściej również z użyciem innych specjalnych interfejsów komunikacyjnych. Obecnie istnieje wiele protokołów i interfejsów przeznaczonych do wymiany danych w sieciach IoT w różnych środowiskach. Każde z tych rozwiązań przeznaczone jest do innych celów i różnią się możliwościami, jednakże większość z nich ma wspólne cechy odróżniające je od protokołów i interfejsów używanych w sieci Internet:

- niskie zużycie energii, co ułatwia projektowanie urządzeń działających przez dłuższy czas na baterii,

- duży zasięg transmisji danych bezprzewodowych, sięgający kilkudziesięciu kilometrów,
- niska przepustowość łącza, rzadko przekraczająca 250 kb/s.

Ważną kwestią jest również fakt, że korzystanie z interfejsów i protokołów komunikacyjnych dla sieci IoT wiąże się z niską prędkością transmisji danych. W kontekście bezpieczeństwa sieci IoT jest to duży problem, ponieważ obsługa mechanizmów zapewniających poufność i integralność transmitowanych danych oraz zaufanie pomiędzy węzłami sieci wiąże się z dużym narzutem przesyłanych danych. W takich sytuacjach często można dostrzec duży spadek wydajności sieci.

3.1. Interfejsy komunikacyjne IoT

W trakcie projektowania sieci IoT najważniejszym czynnikiem wpływającym na wydajność transmisji danych jest wykorzystywany interfejs komunikacyjny. Ze względu na charakter i przeznaczenie takich sieci, często stosuje się w nich technologię LPWAN (ang. *Low Power Wide Area Network*). Technologia ta umożliwia urządzeniom IoT komunikację z wykorzystaniem bezprzewodowego medium transmisji, która charakteryzuje się niskim zużyciem energii oraz transmisją danych na duże odległości.

3.1.1. LoRa

Interfejs LoRa (ang *Long-Range*) jest przeznaczony do radiowej transmisji danych pomiędzy urządzeniami IoT o niskim poborze mocy. Charakteryzuje go niewielka prędkość transmisji danych sięgająca maksymalnie 50 kb/s. Zasięg sieci LoRa na otwartym terenie może sięgać do 28 km [3]. Do komunikacji wykorzystywane są następujące nielicencjonowane pasma częstotliwości radiowych:

- 169 MHz;
- 433 MHz;
- 868 MHz (Europa);
- 915 MHz (Ameryka Północna).

3.1.2. Sigfox

Jednym z najczęściej używanych interfejsów bezprzewodowych do transmisji danych w sieciach IoT jest Sigfox. Technologia Sigfox została zaprojektowana w taki sposób, aby zużycie energii urządzeń było minimalne i umożliwiało pracę na baterii do kilku lat. Dodatkowo interfejs ten umożliwia

transmisję danych na odległość sięgającą 50 km w obszarach wiejskich oraz do 10 km w obszarach zabudowanych [4]. Technologia Sigfox działa w jednym z dwóch pasm częstotliwości radiowej:

- 868 MHz;
- 902 MHz.

Urządzenia korzystające z Sigfox są zdolne transmitować dane z prędkością sięgającą około 0,1 kb/s. Tak niewielka przepustowość oznacza, że nadają się one jedynie do transmitowania takich danych, jak pomiary z różnego rodzaju czujników, natomiast nie znajdą zastosowania przy wymianie większej ilości danych. Dużą zaletą jest zasięg transmisji. Dzięki temu urządzenia wykorzystujące technologię Sigfox są idealne do monitorowania pracy i wykonywania pomiarów w sieciach przemysłowych, natomiast nie znajdą zastosowania przy wymianie bardziej złożonych danych.

3.1.3. XBee

Interfejs XBee jest interfejsem zapewniającym bezprzewodową transmisję danych pomiędzy urządzeniami IoT w paśmie 2,4 GHz. Moduł komunikacyjny XBee możne być podłączony do głównego urządzenia jednym z dwóch interfejsów, co bezpośrednio wpływa na prędkość transmisji danych:

- UART – umożliwia transmisję danych z prędkością 250 kb/s;
- SPI – umożliwia transmisję danych z prędkością 5 Mb/s.

W porównaniu do pozostałych interfejsów dla urządzeń IoT, prędkość transmisji danych zapewniona przez XBee jest najwyższa, jednakże maksymalny zasięg wynosi około 3 km [5]. Oznacza to, że jest to interfejs przeznaczony dla systemów wymagających szybkiej transmisji danych na stosunkowo niewielką odległość.

Tab. 1. Zestawienie interfejsów LPWAN

	LoRa	Sigfox	XBee
Zasięg transmisji (km)	28	Tereny wiejskie: 50 Tereny zabudowane: 10	3
Pasmo częstotliwości (MHz)	169 433 868 915	868 902	2400
Prędkość transmisji (kb/s)	50	0,1	250 (UART) 5000 (SPI)

3.2. Protokoły komunikacyjne IoT

Obecnie istnieje wiele protokołów komunikacyjnych przeznaczonych dla systemów IoT. Często ze względu na środowisko pracy nie ma możliwości, aby podłączyć urządzenia bezpośrednio do sieci Internet. Urządzenia komunikują się wówczas między sobą z wykorzystaniem specjalnych interfejsów komunikacyjnych (rozdział 3.1), a dodatkowo istnieje możliwość komunikowania się tych urządzeń z sieciami zewnętrznymi poprzez tzw. Bramki (ang. *Gateway*). Bramki stosowane są w przypadku każdego z protokołów IoT, a do jednej z ich funkcji należy translacja ramek na postać akceptowalną w sieci Internet, jeżeli protokół IoT nie obsługuje stosu protokołów TCP/IP.

3.2.1. Protokół LoRaWAN

LoRaWAN jest bezprzewodowym protokołem komunikacyjnym przeznaczonym do transmisji danych w rozległych sieciach IoT o niskiej przepustowości oraz dla urządzeń z ograniczonymi zasobami energetycznymi [6]. Protokół ten został zaprojektowany specjalnie dla interfejsu LoRa (punkt 3.1.1).

LoRaWAN ma na celu zapewnienie komunikacji urządzeniom, które według założenia powinny działać przez długi czas na jednej baterii. Sieci korzystające z tego protokołu są sieciami peer-2-peer, a kontakt z siecią Internet możliwy jest poprzez bramki. Nagłówek wykorzystywany przez LoRaWAN ma 13 bajtów.

Cechą charakterystyczną protokołu LoRaWAN jest brak komunikacji bezpośredniej pomiędzy urządzeniami końcowymi. Każda wymiana danych musi odbyć się poprzez serwer. Dodatkowo protokół LoRaWAN ma zaimplementowane szyfrowanie danych z wykorzystaniem 128-bitowych kluczy AES.

3.2.2. Protokół AMQP

Protokół AMQP (ang. *Advanced Message Queuing Protocol*) to protokół przeznaczony do wymiany danych pomiędzy aplikacjami w sposób asynchroniczny, a jego działanie bazuje na kolejkach. Protokół wyróżnia trzy elementy biorące udział w komunikacji:

- Exchange – pośrednik w wymianie wiadomości, obsługuje kolejki i podejmuje decyzje, w których kolejkach umieszczać wiadomości;
- Publisher – tworzy i wysyła wiadomości do Exchange;
- Consumer – klient, który pobiera wiadomości z kolejki.

AMQP jest protokołem asynchronicznym, co oznacza że odczyt wiadomości może nastąpić w dowolnym momencie i nie jest konieczne

nawiązywanie bezpośredniego połączenia pomiędzy dwoma węzłami końcowymi. Publisher w trakcie wysyłania wiadomości ustawia parametry wiadomości, które mogą być wykorzystane przez Exchange do ich obsługi. Nagłówek w protokole AMQP ma 8 bajtów.

Exchange na podstawie atrybutów wiadomości oraz wcześniej definiowanych zasad zwanych wiązaniami (ang. *bindings*) umieszcza wiadomości w odpowiednich kolejkach. Następnie wiadomości są dostarczane do Consumerów, którzy zasubskrybowali daną kolejkę bądź na ich żądanie. Exchange po otrzymaniu potwierdzenia odebrania wiadomości usuwa ją z kolejki, natomiast w przypadku niepowodzenia wiadomość może być zwrócona do Publishera, usunięta bądź przeniesiona do „*dead letter queue*" jeśli jest zainstalowane specjalne rozszerzenie. O podjętej czynności decyduje Publisher w trakcie ustawiania parametrów wiadomości.

Protokół AMQP cechuje wysoka wydajność, dzięki czemu jest w stanie obsłużyć dużą liczbę wiadomości w krótkim czasie. Dodatkowo zapewnione jest w nim bezpieczeństwo poprzez obsługę funkcji uwierzytelniania i szyfrowania. Ponadto protokół ten jest odporny na awarie. Negatywną cechą protokołu AMQP jest wymaganie dotyczące zasobów sprzętowych, w szczególności dla węzła Exchange, co w przypadku węzłów IoT nie zawsze jest możliwe.

3.2.3. Protokół CoAP

CoAP (ang. *Constrained Application Protocol*) jest protokołem działającym podobnie do modelu klient/serwer protokołu HTTP, jednakże węzły pełnią funkcję zarówno klienta, jak i serwera [7]. Każdy węzeł, który chce się skomunikować z innym, pełni funkcję klienta i wysyła zapytanie do drugiego węzła, który jako serwer udziela odpowiedzi. Zapytania wysyłane do serwera są podobne do zapytań HTTP. Wykorzystywane są metody (GET, POST, PUT, DELETE),
a odwoływanie się do zasobów odbywa się z wykorzystaniem URI (ang. *Uniform Resource Identifier*).

CoAP został zaprojektowany specjalnie dla urządzeń o ograniczonych zasobach, w związku z czym wiadomości są skondensowane, a nagłówki mają 4 bajty. Dzięki temu wymagana jest mniejsza przepustowość sieci oraz oszczędzane są zasoby urządzeń. Co więcej, CoAP ma zaimplementowane mechanizmy bezpieczeństwa, takie jak obsługa protokołu DTLS (ang. *Datagram Transport-Layer Security*), który zapewnia szyfrowanie i uwierzytelnianie danych.

3.2.4. Protokół MQTT

Protokół MQTT (ang. *Message Queuing Telemetry Transport*) jest lekkim protokołem komunikacyjnym przeznaczonym dla sieci IoT. MQTT zostało zaprojektowane z myślą o urządzeniach IoT dysponujących niewielkimi zasobami pamięciowymi i obliczeniowymi. Dzięki niskim wymaganiom protokołu w kwestii dotyczącej zasobów, MQTT umożliwia wymianę danych pomiędzy urządzeniami bez większego wpływu na ich wydajność.

Protokół MQTT działa na zasadzie publikacji i subskrypcji. Występują w nim trzy typy urządzeń: MQTT Broker, który jest serwerem pośredniczącym w wymianie danych, MQTT Publisher, który wysyła dane do brokera oraz MQTT Subscriber, który pobiera interesujące go dane do Brokera. Broker przechowuje listę tematów, odnośnie do których może przyjmować i wysyłać wiadomości. Publisher może opublikować swoje dane na dany temat, który jest umieszczany w nagłówku wiadomości, natomiast subscriber może te dane pobrać, jeśli jest zainteresowany tematem. Dzięki temu minimalizowana jest liczba przesyłanych wiadomości.

Protokół MQTT cechuje duża skalowalność, dzięki której możliwe jest przesyłanie danych do wielu odbiorców jednocześnie. Dodatkowo możliwe jest łatwe dodawanie nowych urządzeń do sieci bez konieczności zmiany jej wcześniejszej konfiguracji. Ponadto urządzenia korzystające z MQTT dzięki minimalnej liczbie przesyłanych wiadomości ograniczają w ten sposób zużycie energii do minimum.

Do największych wad protokołu MQTT należy brak mechanizmów bezpieczeństwa. MQTT nie zapewnia poufności ani integralności danych, w związku z czym w celu zapewnienia bezpieczeństwa danych konieczna jest implementacja niezależnych protokołów, takich jak TLS.

3.2.5. Protokół ZigBee

Protokół ZigBee został zaprojektowany dla urządzeń IoT o niskim poborze mocy i pracujących w sieciach, w których komunikacja odbywa się z wykorzystaniem interfejsu XBee. ZigBee wymagania istnienia dwóch typów węzłów: koordynatora, czyli węzła sieciowego odpowiedzialnego za inicjację połączeń, zarządzanie siecią i przesyłanie wiadomości pomiędzy urządzeniami oraz urządzenia końcowego, pełniącego różne funkcje.

ZigBee ma warstwową budowę, gdzie każda z warstw pełni inne funkcje i jest niezależna od innych, a jednocześnie ściśle współpracuje z sąsiadującymi warstwami. Można wyróżnić cztery warstwy: warstwę fizyczną (PHY), warstwę MAC (ang. *Medium Access Control*), warstwę sieciową (NWK) oraz warstwę aplikacji (APL). Protokół ZigBee, dzięki rozbudowanej warstwie NWK, jest w stanie obsłużyć topologię gwiazdy, drzewa oraz mesh.

Protokół ZigBee ma zaimplementowane funkcje kryptograficzne podnoszące poziom bezpieczeństwa sieci. Transmitowane wiadomości zabezpieczane są szyfrowaniem AES z kluczem 128-bitowym. Dodatkowo każde z urządzeń musi przejść autoryzację, aby dołączyć do sieci i uczestniczyć w wymianie danych, co zapewnia budowę zaufanego środowiska już na wczesnym etapie funkcjonowania sieci.

Podsumowanie

We współczesnych sieciach IoT stosuje się wiele różnych rozwiązań, a każde z nich charakteryzują inne właściwości. Wybór odpowiednich technologii i mechanizmów uwarunkowany jest funkcjami, jakie dana sieć ma pełnić.

W kontekście bezpieczeństwa ważne jest, aby sieć już od początku funkcjonowania zapewniała zaufanie pomiędzy węzłami sieci. Z tego powodu konieczne jest wdrożenie wydajnych i skutecznych mechanizmów uwierzytelniania. W zależności od wymagań stawianych sieciom przez administratorów, do których należy między innymi stopnień zautomatyzowania węzłów, możliwy jest wybór różnych mechanizmów oferujących różne funkcje. Mechanizmy takie mogą obejmować uwierzytelnianie z wykorzystaniem kontekstów, haseł oraz kryptografii asymetrycznej.

Kolejnym ważnym aspektem jest zapewnienie poufności transmitowanych danych. W tym celu zazwyczaj korzysta się z kryptografii symetrycznej ze względu na wymaganą mniejszą moc obliczeniową i mniejsze zasoby pamięciowe niż w przypadku kryptografii asymetrycznej. Stosowanie kryptografii symetrycznej wiąże się jednak z problemem bezpiecznego rozpowszechnienia klucza symetrycznego, szczególnie gdy konieczne jest zapewnienie jednego klucza dla wielu węzłów. Z tego powodu konieczne jest wdrożenie odpowiednio zaprojektowanego skalowalnego systemu dystrybucji kluczy symetrycznych.

Istnieją dwa podejścia dotyczące dystrybucji kluczy symetrycznych: KDC oraz KTC. Każde z tych rozwiązań skupia się na innych aspektach. KDC jest rozwiązaniem scentralizowanym, gdzie najważniejsze operacje kryptograficzne wykonywane są na węźle centralnym. KTC jest podejściem zdecentralizowanym, gdzie każdy z kluczy jest generowany na węzłach końcowych, a węzeł centralny odpowiada jedynie za przekazanie gotowego klucza do innych węzłów, a brak konieczności generowania klucza odciąża węzeł centralny i umożliwia szybsze obsługiwanie kolejnych żądań.

Ostatnią kwestią poruszaną w artykule jest transmisja danych pomiędzy węzłami IoT. Ze względu na ograniczony dostęp do zasobów energetycznych urządzenia wykorzystują specjalne interfejsy komunikacyjne i protokoły wymiany danych. Każde z tych rozwiązań cechuje inny zasięg oraz prędkość transmisji danych, w związku z czym wybór odpowiednich rozwiązań

podyktowany jest środowiskiem, w jakim działa sieć oraz zadaniami, jakie mają w ramach takiej sieci być realizowane.

Literatura

[1] Needham R. M., Schroeder M. D., *Using encryption for authentication in large networks of computers*, Communications of the ACM, vol. 21, no. 12, 1978, pp. 993-999.

[2] Barker E. and Baker W., *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*, NIST Special Publication 800-57 Revision 1. May, 2019.

[3] Jovalekic N., Drndarevic V., Pietrosemoli E., Darby I., Zennaro M., *Experimental Study of LoRa Transmissionover Seawater*, Sensors, 18 (9), 2853, 2018.

[4] Augustin A., Yi J., Clausen T., Townsley W. M., *A Study of LoRa: Long Range & Low Power Networks for the Internet of Things*, Sensors, 16 (9), 1466, 2016.

[5] Maciaszczyk R., *Transmisja danych z pojazdów bezzałogowych z wykorzystaniem modułów XBee*, Pomiary Automatyka Kontrola, R. 58, nr 2, 2012, s. 656-658.

[6] Farrell S., [RFC 8376], *Low-Power Wide Area Network (LPWAN) Overview*, 2018.

[7] Shelby A., Hartke K., Bormann C., [RFC 7252], *The Constrained Application Protocol (CoAP)*, 2014.

Secure and efficient data exchange in Internet of Things networks – technology review

ABSTRACT: IoT devices are often accompanied by numerous hardware constraints, such as limited computing power, limited memory resources, and low network bandwidth. All these components have a significant impact on the difficulties in ensuring the security of IoT networks. For this reason, various solutions designed specifically for IoT devices have been developed to increase the level of security of such devices. The paper reviews the most popular solutions used in IoT networks that minimize problems caused by numerous limitations.

KEYWORDS: IoT, IoT network security, key distribution, lightweight data exchange protocols, IoT communication interfaces

Praca wpłynęła do redakcji: 15.05.2023 r.

Recenzenci artykułów czasopisma naukowego PRZEGLĄD TELEINFORMATYCZNY

Lata 2021-2022

Aleksiejuk Mikołaj	Instytut Podstawowych Problemów Techniki PAN
Ambroziak Tomasz	Wydział Transportu, Politechnika Warszawska
Gogołek Włodzimierz	Wydział Dziennikarstwa, Informacji i Bibliologii, Uniwersytet Warszawski
Graniszewski Waldemar	Politechnika Warszawska, Wydział Elektryczny
Jakubowski Jacek	Wydział Elektroniki, Wojskowa Akademia Techniczna
Jarmakiewicz Jacek	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy
Jung Leszek	Instytut Sztuki i Nauk Technicznych, Społeczna Akademia Nauk
Korbel Piotr	Instytut Elektroniki, Politechnika Łódzka
Kosiński Jerzy	Wydział Dowodzenia i Operacji Morskich, Akademia Marynarki Wojennej
Liderman Krzysztof	Wydział Cybernetyki, Wojskowa Akademia Techniczna
Terebiński Bartłomiej	Wydział Wojskowy, Akademia Sztuki Wojennej
Weydman Romuald	MILSTAR
Życzkowski Marek	Instytut Optoelektroniki, Wojskowa Akademia Techniczna

Information for Authors – rules of papers preparation and reviewing for TELEINFORMATICS REVIEW

The *Teleinformatics Review* is devoted to the publication of original research results in fields of science including, but not limited to: computer science, telecommunication, signal processing, network systems, automation and robotics, etc., which have not been published elsewhere in their entirety or considerable part. If a submitted paper is a part of another published work, e.g. a doctoral dissertation, a postdoctoral thesis, etc., the source work should be included in the list of literature and the editorial office must be informed about it.

In order to publish a paper in the Teleinformatics Review it is necessary to submit it to the editorial office in an electronic form (and possibly its printed copy, one-sided, legible, on white A4 sheets) according to the given template. Only original works in English or Polish will be accepted. The text of the paper should be prepared in the format of Microsoft Word editor (versions 2003 or 2010 are suggested). Appropriate templates can be downloaded from website review.ita.wat.edu.pl (or przeglad.ita.wat.edu.pl). The electronic version submitted to the editorial office should contain a source file of the paper in DOC or DOCX format, with all figures and tables being inserted. The editorial office does not rewrite the text neither make drawings. In addition to the mentioned source file, all figures should be delivered in commonly used image formats (preferably as EPS, JPG, TIFF, or others).

Papers to be published in the Teleinformatics Review are subject to initial acceptance by the editorial office and then are subject to review by two external reviewers. Reviewers and authors do not know each other personal data. The content of the review will be available at the editorial office. If one review is negative (or imprecise) then a third reviewer may be appointed. If both reviews are negative the paper is rejected. If the review indicates a necessity of some corrections, the author must consider all of them and resubmit the improved paper by the determined deadline.

The volume of a submitted paper generally not exceed 20 pages of typescript A4. A deviation from this rule requires agreement of the editorial office. Except the last page, no more than 10% of any page within the paper can be left empty. Figures must be numbered and described below them as well as tables must be numbered and described at the top of them. The literature should hold the form given in the template.

The authors are obliged to submit a statement to the editorial office on the percentage contribution to the creation of the accepted paper, confirming the lack

of prior publication of such a work, or a public speech on the subject at a conference or symposium.

The editorial board reserves rights to introduce minor editorial changes to the content of paper without consulting the author. The editorial office insists that no special formatting should be used, which would be inconsistent with the template.

Papers printed in the Teleinformatics Review and their abstracts are placed in the national database of Polish technical journals BazTech as well as on the INDEX COPERNICUS website. Additionally, the papers will be available in the electronic PDF form on website review.ita.wat.edu.pl.

Publication in the Teleinformatics Review does not involve any costs for authors. The editorial office does not charge for submitting, reviewing, preparing for publication and publishing the work. The publication of a paper in the Teleinformatics Review is tantamount to transfer of authors' property rights for publication to the publisher, i.e. the Military University of Technology. By submitting a paper for publication in the Teleinformatics Review, the author agrees, for publication purposes, to the processing by the editorial office the author's name, email address, affiliation, and other contact details.

The editorial office does not return received materials.

The editorial office does not pay fees for papers publishing.

The editor-in-chief may refuse to publish a paper in the following cases:

- if the content of the paper violates the law (principles of secrecy protection, press law, copyright law, etc.) or good manners;
- the author does not agree to introduce all necessary corrections proposed by the editorial board or reviewers;
- the text and illustrative material submitted by the author does not meet the technical requirements given in this document or the template.

Informacje dla autorów – zasady przygotowania tekstu i recenzowania artykułów do PRZEGLĄDU TELEINFORMATYCZNEGO

W Przeglądzie Teleinformatycznym zamieszczane są oryginalne artykuły z dziedzin: *informatyka, telekomunikacja, przetwarzanie sygnałów, systemy sieciowe, automatyka i robotyka* oraz pokrewnych, niepublikowane dotychczas w całości lub w znaczącej części. Jeśli nadesłana praca stanowi część innej opublikowanej pracy, np. pracy doktorskiej, habilitacji, etc., to źródło powinno być umieszczone w spisie literatury, a redakcja powinna być o tym poinformowana.

W celu opublikowania artykułu w *Przeglądzie* niezbędne jest dostarczenie do redakcji treści artykułu w postaci **elektronicznej** według podanego szablonu i ewentualnie jednego egzemplarza wydrukowanego (jednostronnie, czytelnie, na białym papierze formatu A4). Przyjmowane są tylko oryginalne prace w języku angielskim lub polskim. Tekst artykułu powinien być przygotowany w formacie edytora Microsoft Word (wersja 2003 lub 2010 jest zalecana). Szablony dla artykułów są dostępne w pliku na stronie przeglad.ita.wat.edu.pl (lub review.ita.wat.edu.pl). Przekazane do redakcji materiały powinny zawierać plik źródłowy w formacie DOC lub DOCX, z wstawionymi rysunkami. Redakcja nie przepisuje tekstów i nie wykonuje rysunków. Dodatkowo należy dostarczyć pliki źródłowe rysunków (najlepiej w formacie EPS, JPG, TIFF lub innym powszechnie używanym).

Artykuły przeznaczone do opublikowania w *Przeglądzie* podlegają wstępnej ocenie przez redaktora działu, a następnie podlegają recenzji przez dwóch zewnętrznych recenzentów. Recenzenci i autorzy nie znają swoich danych personalnych. Z treścią recenzji można zapoznać się w redakcji. Jeśli jedna z recenzji jest negatywna (lub nieprecyzyjna), może być powołany trzeci recenzent. Jeśli dwie recenzje są negatywne, artykuł jest odrzucany. Jeśli z recenzji wynika konieczność dokonania poprawek w treści artykułu, to autor jest zobowiązany do ich rozpatrzenia i dostarczenia do redakcji poprawionej wersji artykułu, w terminie ustalonym przez redakcję.

Objętość artykułu zasadniczo nie powinna przekroczyć 20 stron maszynopisu A4. Odstąpienie od tej zasady wymaga uzgodnień z redakcją *Przeglądu*. Na stronach tekstu artykułu nie może być pozostawione więcej niż 10% pustego miejsca, za wyjątkiem ostatniej strony. Rysunki należy numerować i opatrzyć (pod spodem) wyczerpującym podpisem. Tabele również muszą być numerowane (tytuł nad tabelą). Literatura może być uszeregowana alfabetycznie oraz powinna mieć postać jak w szablonie.

Autorzy są zobligowani do złożenia w redakcji oświadczenia autorskiego o wkładzie procentowym w powstanie artykułu, braku wcześniejszej publikacji artykułu w przedstawionej formie lub wystąpieniu publicznym na ten temat na konferencji lub sympozjum.

Redakcja zastrzega sobie prawo wprowadzenia niewielkich redakcyjnych zmian w treści artykułu bez konsultacji z autorem. Redakcja nalega, aby **nie stosować** żadnego specjalnego formatowania i **trzymać się ściśle** ustaleń zawartych w szablonie.

Streszczenia i pełne teksty artykułów drukowanych w *Przeglądzie* zamieszczane są w krajowej bazie danych o zawartości polskich czasopism technicznych BazTech oraz na platformie INDEX COPERNICUS. Opublikowane w *Przeglądzie* artykuły będą także w całości udostępnione w internetowej wersji (format PDF) czasopisma, pod adresem przeglad.ita.wat.edu.pl (lub review.ita.wat.edu.pl).

Publikacja w *Przeglądzie* nie wiąże się z żadnymi kosztami dla autorów. Redakcja nie pobiera opłat za zgłoszenie, przygotowanie do druku, recenzję czy publikację pracy. Przekazanie artykułu do publikacji w *Przeglądzie* jest równoznaczne z przekazaniem autorskich praw majątkowych do publikacji na rzecz wydawcy, tj. Wojskowej Akademii Technicznej. Przekazując artykuł do publikacji w *Przeglądzie* autor zgadza się na przechowywanie i przetwarzanie przez redakcję, w celach publikacyjnych, imienia, nazwiska, adresu e-mail i afiliacji.

Redakcja nie zwraca materiałów dostarczonych do redakcji.

Redakcja nie przewiduje honorariów za opublikowanie artykułu.

Redaktor naczelny może odmówić opublikowania artykułu w przypadku, gdy:

- treści zawarte w materiałach naruszają prawo (zasady ochrony tajemnicy, prawo prasowe, prawo autorskie itp.) lub dobre obyczaje;
- autor nie zgadza się na wprowadzenie wszystkich koniecznych poprawek zaproponowanych przez redakcję lub recenzentów;
- tekst i materiał ilustracyjny złożony przez autora nie spełnia wymagań technicznych podanych w niniejszym dokumencie i szablonie.