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.

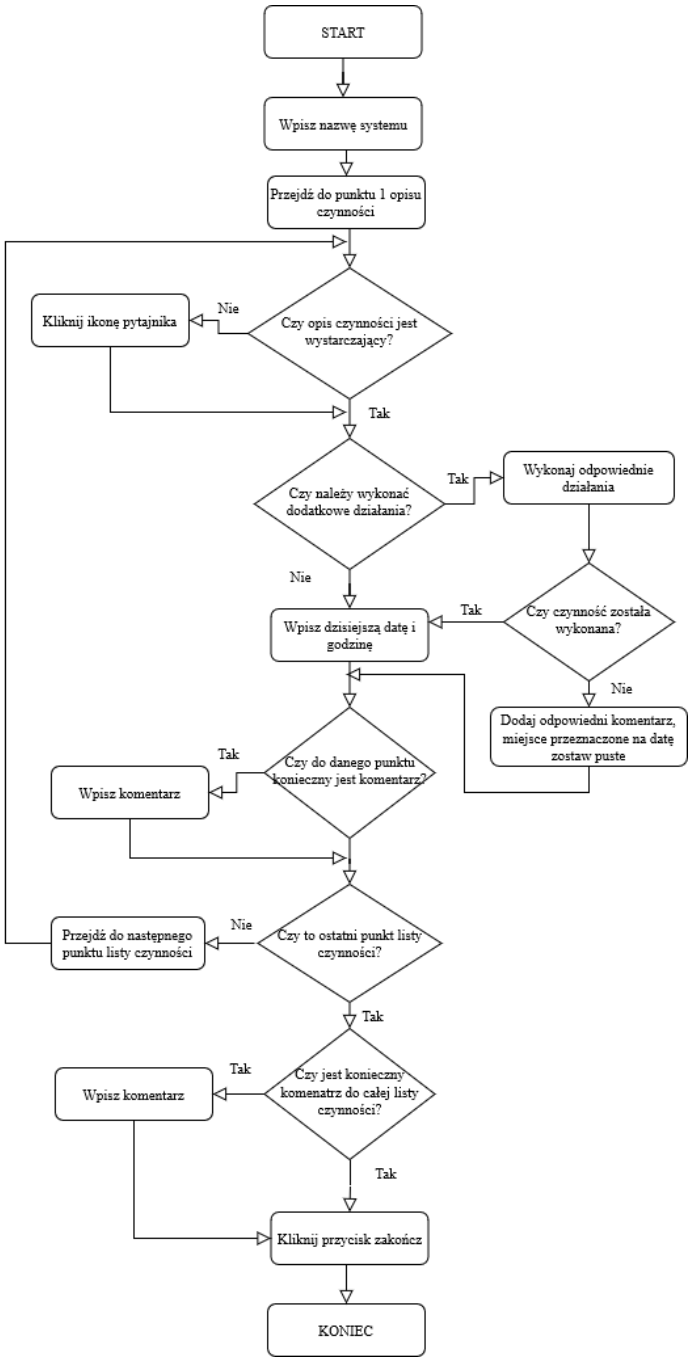
2.1. Jeżeli nie jest konieczne podjęcie żadnych działań (patrz ostatnie zdanie opisu czynności), należy wpisać dzisiejszą datę.
2.2. Jeśli opis czynności jest niewystarczający, kliknij w ikonę pytajnika po prawej stronie. Zostanie otwarte okno z szerszym opisem.
2.3. Jeśli konieczne jest wykonanie dodatkowych 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.

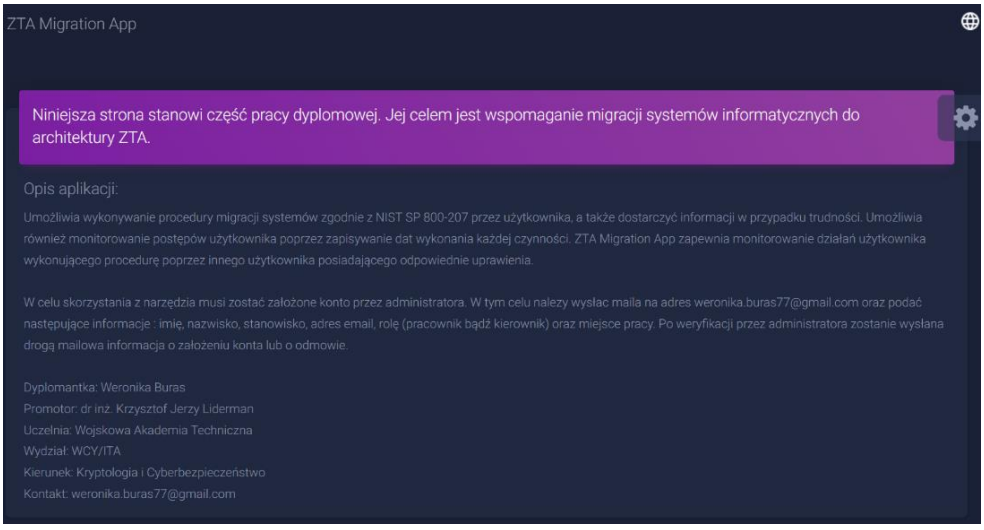


Rys. 3. Diagram sekwencji przedstawiający sposób użycia listy czynności

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:

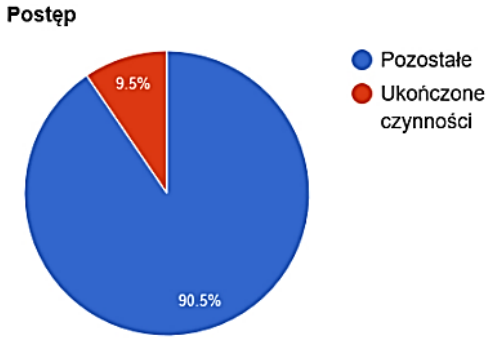
- Narzędzie Diagrams.net [4] − darmowe rozwiązanie opracowane przez JGraph Ltd., które umożliwia tworzenie diagramów między innymi typu UML, sieciowego czy schematów blokowych.
- Narzędzie SQL Server Management Studio − środowisko opracowane przez firmę Microsoft, które między innymi umożliwia dostęp,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