Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215903

Opportunities and threats associated with the use of open source software in an organization

Szanse i zagrożenia związane z wykorzystywaniem oprogramowania otwartoźródłowego w organizacji

David CYBULSKI
Akademia Sztuki Wojennej
ORCID: 0009-0003-9195-4407
E-mail: d.cybulski@doktorant.akademia.mil.pl

Abstract

The article analyzes the opportunities and threats associated with the implementation of open source software in organizations, with the aim of providing a comprehensive picture of the benefits and risks involved.

The study used literature review and case study methods. In addition, secondary research based on existing data analysis was conducted, which allowed for verification of the popularity of the open source applications.

The results indicate that open source software can reduce licensing costs and increase the flexibility and innovation od organizations. Users have full control over the source code, which allows them to adapt the software to the specific needs of the entity. In addition, the open nature of the software facilitates faster detection and correction of errors and greater independence form suppliers. At the same time, challenges have been identified, including application security, lack of technical support, and the need for qualified personnel for implementation and maintenance. In practice, effective use depends on conscious risk management and implementation strategy.

The conclusions emphasize that although open-source solutions offer significant benefits, their safe and effective use requires proper planning and investment in competencies.

Keywords
open-source, foss, cybersecurity

Streszczenie

Artykuł analizuje szanse i zagrożenia związane z wdrażaniem oprogramowania otwartoźródłowego w organizacjach, mając na celu dostarczenie kompleksowego obrazu korzyści i ryzyk z tym związanych.

W badaniu zastosowano metody przeglądu literatury oraz analizy przypadków. Dodatkowo przeprowadzono badania wtórne oparte na analize danych zastanych, co pozwoliło na weryfikację popularności wykorzystywania aplikacji otwortoźródłowych.

Wyniki wskazują, iż oprogramowanie otwartoźródłowe może obniżyć koszty licencji oraz zwiększyć elastyczność i innowacyjność w organizacji. Użytkownicy mają pełną kontrolę nad kodem źródłowym, co pozwala na dostosowanie oprogramowania do specyficznych potrzeb podmiotu. Ponadto otwarty charakter oprogramowania sprzyja szybszemu wykrywaniu i naprawianiu błędów oraz większej niezależności od dostawców. Jednocześnie zidentyfikowano wyzwania związane m.in. z bezpieczeństwem aplikacji, brakiem wsparcia technicznego oraz koniecznością posiadania wykwalifikowanego personelu do wdrożenia i utrzymania. W praktyce efektywność wykorzystanai zależy od świadomego zarządzania ryzykiem i strategii wdrożeniowej.

Wnioski podkreślają, że choć otwartoźródłowe rozwiązania oferują istotne korzyści, ich bezpieczne i efektywne wykorzystanie wymaga odpowiedniego planowania oraz inwestycji w kompetencje.

Słowa kluczowe

open-source, foss, oprogramowanie otwartoźródłowe, cyberbezpieczeństwo

Wprowadzenie

W dobie dynamicznego rozwoju technologii informatycznych aplikacje otwartoźródłowe (ang. open-source) coraz częściej zyskują na znaczeniu w funkcjonowaniu współczesnych organizacji, oferując atrakcyjną alternatywę dla rozwiązań komercyjnych, bądź stanowiąc wypełnienie dotychczasowej luki rynkowej. Wybór niniejszego tematu podyktowany jest rosnącą popularnością narzedzi open-source, które niosą ze sobą znaczące korzyści, jak i potencjalne zagrożenia, zwłaszcza w kontekście bezpieczeństwa, wsparcia technicznego i kosztów utrzymania. Zarówno przedsiębiorstwa, jak i organy administracji państwowej coraz częściej sięgają po narzędzia o otwartym kodzie źródłowym ze względu na ich niższe koszty, elastyczność czy potencjał do innowacji. Jednakże adaptacja oprogramowania tego typu do potrzeb danego podmiotu niesie ze sobą również istotne wyzwania i ryzyka, związane między innymi z aspektami bezpieczeństwa, wsparciem technicznym czy licencjonowaniem produktów. Krytyczna analiza literatury wskazuje, iż choć wiele źródeł podkreśla ekonomiczne i techniczne zalety otwartego oprogramowania, istnieje niedobór kompleksowych analiz dotyczących szans i ryzyk tej technologi w realiach organizacyjnych.

Celem artykułu jest identyfikacja i ocena szans oraz zagrożeń związanych z wykorzystywanem oprogramowania otwartoźródłowego w organizacjach. Pytania badawcze: Jakie korzyści finansowe i operacyjne przynosi wdrożenie

narzędzi open-source? Jakie są kluczowe zagrożenia open-source i w jaki sposób można im przeciwdziałać? Forumłowana hipoteza zakłada, iż korzyści z implementacji open-source przewyższają ryzyka pod warunkiem odpowiedniego zarządzania i świadomości organizacyjnej.

W badaniach zastosowano metody przeglądu literatury, analizy przypadków oraz przeprowadzono badania wtórne oparte na analizie danych zastanych. Artykuł został podzielony na następujące części: wprowadzenie, definicja i charakterystyka wolnego oprogramowania, zalety wolnego oprogramowania, wady wolnego oprogramowania, znaczenie oprogramowania otwartoźródłowego dla podmiotów admininstracji publicznej i środowisk biznesowych oraz podsumowanie.

Definicja i charakterystyka wolnego oprogramowania

Jak trafnie wskazał W. Barcikowski „wolne i otwarte (o otwartych źródłach) oprogramowanie (ang. Free and Open Source Software - FOSS) jest rodzajem oprogramowania rozpowszechnianego na zasadzie specyficznej licencji dającej użytkownikowi prawo do jego bezpłatnego użytkowania”[1]. Cechami charakterystycznymi dla przedmiotowego typu oprogramowania jest jego dostępność dla szerokiego grona odbiorców, czy też zwyczajowy sposób jego utrzymania opierający się na społeczności wolontariuszy dedykujących swój czas celem rozwijania tejże usługi dla dobra ogółu. Podstawą oprogramowania otwartoźródłowego jest to, iż jego kod źródłowy pozostaje dostępny do wglądu i modyfikacji (w zależności od licencji na jakiej jest dystrybuowane) przez zainteresowane osoby. Powyższe wiąże się jednak z wieloma restrykcjami, szansami czy też wprost zagrożeniami.

Należy nadmienić, iż nierzadko oprogramowanie typu open-source stanowi podstawy bardziej zaawansowanych projektów, w tym i komercyjnych, na których opiera się wiele dziedzin życia społecznego. Za przykład posłużyć tu mogą usługi takie jak:

- Linux – rodzina systemów operacyjnych opartych na jądrze Linux, zaprojektowana jako wolne i otwarte oprogramowanie. Stosowany w szerokim spektrum środowisk – od serwerów, superkomputerów, przez routery, czy urządzenia Internetu Rzeczy (ang. Internet of Things, IoT);
- Android – otwartoźródłowa platforma oparta na jądrze Linux oraz zestawie bibliotek i usług dostarczających zestandaryzowane środowisko uruchomieniowe dla aplikacji. System Android pełni kluczową rolę w globalnym runku technologii mobilnych, zapewniając skalowalne środowisko aplikacyjne oparte na architekturze komponentowej;
- Firefox – otwartoźródłowa przeglądarka internetowa rozwijana przez Mozilla Foundation. Architektura Firefox oparta jest na silniku renderującym Gecko i wieloprocesowym modelu wykonywania. Projekt stanowi implementację klienta protokołów i standardów sieciowych definiowanych przez World Wide Web Consortium (W3C) oraz Internet Engineering Task Force (IETF), koncentrując się na zgodności z otwartymi specyfikacjami;
- Nginx – wysokowydajny, asynchroniczny serwer pośredniczący World Wide Web (WWW). Podstawowym założeniem projektu jest minimalizacja kosztów

[1] W. Barcikowski, Wykorzystanie otwartego oprogramowania w informatycznych systemach zarządzania [w:] “Nowoczesne systemy zarządzania” 2012, s. 338.

obsługi operacji wejścia-wyjścia poprzez zastosowanie nieblokujących mechanizmów asynchronicznych dostępnych w systemach Unix;
- MySQL/MariaDB/PostgreSQL – klasy systemów zarządzania bazami danych, różniące się modelem architektury i zakładanymi scenariuszami użycia. MySQL oraz MariaDB bazują na klasycznym modelu klient-serwer i są szeroko wykorzystywane w systemach transakcyjnych o umiarkowanym stopniu złożoności. PostgreSQL impelmentuje model obiektowo-relacyjny zgodny ze standardem SQL oraz umożliwia rozszerzanie funkcjonalności o typy danych, funkcje i procedury, co predestynuje go do zastosowań analitycznych i korporacyjnych.

W obecnym, cyfrowym świecie mimo częstej nieświadomości użytkownika końcowego opisane powyżej usługi otwartoźródłowe stanowią podstawę funkcjonowania dzisiejszego cyfrowego świata, bez których trudno by sobie wyobrazić funkcjonowanie praktycznie jakiejkolwiek usługi cyfrowej, w tym bankowości (nie tylko elektronicznej), telefonii komórkowej, usług internetowych, czy świata e-commerce. Pierwszy z przedstawionych przykładów stanowi choćby podstawę środowisk serwerowych na świecie (62,4% - 70,4%)[2], drugi odpowiada za 72% całości globalnego rynku smartfonów[3], a trzeci stanowi 4 największą przeglądarkę internetową na świecie[4].

Zalety wolnego oprogramowania

Najczęściej wymianianą korzyścia z wykorzystywania oprogramowania otwartoźródłowego przez różnego typu organizacje jest możliwość korzystania z takowego oprogramowania jest jego cena, a w zasadzie brak kosztów licencyjnych (w zależności od licencji). Oprogramowanie open-source jest dostępne bezpłatnie, co pozwala organizacjom na znaczne oszczędności w budżecie IT. Jest to jeden z kluczowych aspektów, który działania znacząco na korzyść oprogramowania typu FOSS, w szczególności dla administracji państwowej oraz mikro, małych i średnich przedsiębiorstw. Jak wskazuje ankieta z raportu The Linux Foundation 46% ankietowanych wskazuje, iż wykorzystywanie oprogramowania *open-source* w organizacji jest tańsze co najmniej dwukrotnie względem wytworzenia podobnych projektów wewnętrznie[5].

Jedną z fundamenetalnych zalet aplikacji otwartoźródłowych dla organizacji, która potencjalnie mogłaby bądź chciałaby taką usługę wdrożyć na swój poczet jest możliwość przejrzystości i audytowalności kodu, przez daną organizację bądź niezależne podmioty. Powyższe sprawia, iż podmiot zainteresowany wdrożeniem wzmiankowanego rozwiązania ma możliwość niezależnego upewnienia się, iż aplikacja działa w określony, akceptowalny przez odbiorcę sposób. Ponadto obiektywni eksperci oraz pasjonaci właściwi w sprawach danej aplikacji mogą również dokonać weryfikacji jej funkcjonalności. Przejrzystość i audytowalność kodu sprawia, iż możliwym staje się prowadzenie

[2] S. Korac i in., Ransomware: Analysis and Evaluation of Live Forensic Techniques and the Impact on Linux based IoT Systems [w:] 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Edinburgh Napier University 2024, s. 1.
[3] A. Gómez, A. Muñoz, Deep Learning-Based Attack Detection and Classification in Android Devices [w:] Electronics 2023 (12), University of Malaga 2023, s. 1.
[4] Browser Market Share Report for 2025 Q3, Cloudflare 2025, https://radar.cloudflare.com/reports/browser-market-share-2025-q3 [dostęp: 25.11.2025].
[5] H. Chesbrough, Measuring the Economi Value of Open Source, The Linux Foundation 2023, s. 15.

dogłębnych analiz wdrażanego do własnej instrastruktury rozwiązania. Stoi to wprost w kontrze do aplikacji charakteryzujących się zamkniętym kodem źródłowym.

Jednym z niedawnych zaś bardzo medialnych doniesień o nieautoryzowanej możliwości ingerencji producenta w systemy zakupione przez klientów są choćby pozyskiwane dla Sił Zbrojnych Rzeczypospolitej Polskiej samoloty wielozadaniowe F-35 produkcji amerykańskiej, wobec których w krajach członkowskich Unii Europejskiej zaistniało wiele obaw o możliwość występowania tzw. funkcji „kill-switch" tychże systemów (możliwość zdalnego unieruchomienia maszyny przez producenta). Takie obawy w szczególności wyrażane były m.in. przez Królestwo Niderlandów[6].

Innym przykładem ryzyka występowania tzw. funkcji „kill-switch" lub „backdoor"[7] w oprogramowaniu o zamkniętym kodzie źródłowym jest - poruszane przy obecnych próbach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa[8] - wykorzystywanie w Unii Europejskiej (w tym w Polsce) urządzeń i systemów chińskiej firmy Huawei. Rozwiązania te m.in. ze względu na swoją stosunkowo niską cenę wykorzystywane są w podmiotach takich jak administracja państwowa oraz operatorzy infrastruktury krytycznej[9]. Firma Huawei znana jest ze swoich praktyk agresywnego lobbyingu, na rzecz silnej obecności produktów chińskich (w tym Huawei) w państwach Unii Europejskiej[10], jednocześnie istnieje silna obawa, iż produkty te mogą posiadać ww. funkcje „backdoor" lub „kill-switch" pozostające pod kontrolą Chińskiej Republiki Ludowej[11]. Funkcje takie jak „backdoor" mogą być zastosowane m.in. do działań cyberwywiadowczych, szczególnie o podłożu państwowym i w przypadku, gdy celem jest podmiot z zakresu administracji państwowej[12]. Z tego względu toczy się obecnie dyskusja na temat ewentualnego uznania w Polsce m.in. firmy Huawei za dostawcę wysokiego ryzyka (zgodnie z procedowaną nowelizacją Ustawy), aby uniemożliwić kluczowym podmiotom (energetyka, sektor bankowy, telekomunikacja etc.) wykorzystywanie technologii tego producenta[13].

---

[6] Beantwoording Kamervragen van lid Nordkamp over 'kill switch', Ministerstwo Obrony Narodowej Królestwa Niderlandów 2025, https://www.rijksoverheid.nl/documenten/kamerstukken/2025/03/25/beantwoording-kamervragen-van-lid-nordkamp-over-kill-switch-in-de-f-35 [dostęp: 26.11.2025].

[7] Backdoor – celowo lub niejawnie pozostawionych mechanizm umożliwiający obejście standardowych procedur uwierzytelniania w celu uzyskania nieautoryzowanego dostępu do systemu.

[8] Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, druk nr 1955, Kancelaria Sejmu RP 2025, https://www.sejm.gov.pl/sejm10.nsf/druk.xsp?nr=1955 [dostęp: 29.11.2025].

[9] W rozumieniu art. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007, Nr 89, poz. 590 z późn. zm.).

[10] M. Pollet, European Commission backlists groups lobbying for Huawei, Politico 2025, https://www.politico.eu/article/european-commission-blacklists-lobby-groups-tied-to-huawei/ [dostęp: 29.11.2025].

[11] B. Pancevski, U.S. Officials Say Huawei Can Covertly Access Telecom Networks, The Wall Street Journal 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256 [dostęp: 29.11.2025].

[12] G. Pilarski, Przegląd współczesnych zagrożeń w cyberprzestrzeni, „Problemy Techniki Uzbrojenia" 2023, t. 167, nr. 5, , s. 100.

[13] A. Pantak, Czy Polskę czeka spór z Huawei? Chodzi o projekt nowych przepisów o cyberbezpieczeństwie, Gazeta Prawna 2025, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/10562128,czy-polske-czeka-spor-z-huawei-chodzi-o-projekt-nowych-przepisow-o-cy.html [dostęp: 29.11.2025].

Następną z zalet wynikającą z przejrzystości i audytowalności kodu przez każdego użytkownika jest możliwość sprawnego wyszukiwania oraz niwelowania zidentyfikowanych podatności i błędów konfiguracyjnych przez zaangażowaną społeczność osób utrzymujących wskazane rozwiązanie oraz entuzjastów[14]. Powyższe daje potencjalną możliwość szybszej reakcji niż przy kodzie zamknięto-źródłowym na zidentyfikowaną lukę bezpieczeństwa, pozwalając na jej mitygację w stosunkowo krótkim czasie. Dana możliwość sprawia, iż użytkownicy i entuzjaści nierzadko mogą zidentyfikować podatność jeszcze przed jej nieuprawnionym wykorzystaniem przez potencjalnego adwersarza. Jak wynika z raportu The Linux Foundation z 2024 roku 68% respondentów ankiety badawczej uważa, iż aplikacje o otwartym kodzie źródłowym są bardziej bezpieczne, niż ich odpowiedniki o zamkniętym kodzie źródłowym[15].

Oprogramowanie otwartoźródłowe wyróżnia się również możliwością dowolnej omdyfikacji i dostosowywania kodu źródłowego aplikacji do specyficznych potrzeb organizacji wdrażającej. Użytkownicy ze względu na specyfikę FOSS mają pełny dostęp do kodu źródłowego, co pozwala nie tylko na poprawę istniejących funkcji, ale także na dodawanie nowych, unikalnych rozwiązań odpowiadających konkretnym wymaganiom biznesowym. Dzięki temu każda organizacja może optymalizować i rozwijać oprogramowanie w sposób najbardziej efektywny dla swoich procesów, co zwiększa elastyczność i konkurencyjność. Dodatkowo, zmodyfikowane wersje mogą być współdzielone w ramach społeczności open-source, co sprzyja ciągłemu doskonaleniu i innowacjom. Taka otwartość i współpraca w rozwoju oprogramowania stanowi istotną przewagę nad systemami zamkniętymi, gdzie modyfikacje są ograniczone lub niemożliwe.

Możliwość uniezależnienia się od pewnych środowisk korporacyjnych, których to coraz większa integracja wewnętrzna jednocześnie niejako zamyka organizacje je wykorzystujące w ramach danego zestawu produktów, również stanowi istotną zaletę rozwiązań typu open-source. Sprawia to, iż z czasem mimo pojawienia się ewentualnej potrzeby zmiany usługi na inną (np. poprzez brak kluczowych funkcji, koszty, organiczenia licencyjne etc.) przejście takie staje się finalnie nieopłacalne względem istniejących potrzeb biznesowych, a podmiot szukający zmiany musi pozostać przy dotychczasowych rozwiązaniach. Idealnymi przykładami zjawiska tzw. „vendor lock-in" są: środowisko usług Google, Microsoft Office oraz ekosystem urządzeń i usług firmy Apple[16].

Jednym z istotnych przykładów chęci uniezależnienia się od narastającego oligopolu technologicznego jest niedawne przejście niemieckiego landu Szlezwik-Holsztyn z rozwiązań m.in. firmy Microsoft na alternatywy otwartoźródłowe, w tym system operacyjny Linux[17]. Skutkiem tejże decyzji jest konieczność zmiany systemu operacyjnego oraz innych usług teleinformatycznych na ok. 30 000 stacjach roboczych urzędników niemieckiego landu. Jest to zbieżne z odczuciami respondentów, którzy wskazują, iż dwoma

[14] E. Sesterhenn, J. Schneeweisz, M. Vervier, Source Code Audit on Git for Open Source Technology Improvement Fund (OSTIF), X41 D-SEC 2025, s. 4 i n.
[15] 2024 Global Spotlight Insights Report, The Linux Foundation 2024, s. 6.
[16] A. Zeeuw i in., The orchestrated digital inequalities of the IoT: How vendor lock-in hinders and playfulness creates IoT benefits in every life, "New Media & Society" 2024, vol. 26, issue 10, s. 5668 i n.
[17] P. Makowiec, Przełomowa decyzja niemieckiego landu, „Chcemy cyfrowej niezależności", CyberDefence24 2024, https://cyberdefence24.pl/cyberbezpieczenstwo/przelomowa-decyzja-niemieckiego-landu-chcemy-cyfrowej-niezaleznosci [dostęp: 29.11.2025].

głównymi czynnikami rozwoju oprogramowania otwartoźródłowego powinno być tworzenie alternatyw dla komercyjnych rozwiązań (49%) oraz implementacja przez administrację państwową narzędzi otwartoźródłowych (40%)[18]. Z resztą należy nadmienić, iż nie jest to odosobniony przypadek, a kolejnym przykładem może być choćby Francuska Żandarmeria Wojskowa wykorzystująca autorską dystrybucję systemu operacyjnego Linux o nazwie „GendBuntu”[19]. Jednocześnie coraz częściej mówi się o stworzeniu europejskiego systemu operacyjnego „EU OS”, który miałby bazować na systemie Linux (obecnie amerykańskiej dystrybucji systemu Linux o nazwie Fedora Linux)[20].

Kolejnym plusem wykorzystywania oprogramowania otawrtoźródłowego jest zazwyczaj wynikające z tego tytułu mniej restrykcyjne podejście do zasad licencjonowania za wykorzystywanie produktu. Czynnik ten przy oprogramowaniu otwartoźródłowym zwyczajowo jest kwestią niemal marginalną lub wprost nieistniejącą (usługi otwartoźródłowe udostępnianie i dystrybuowane bez licencji). Najczęstsze licencje do używania, modyfikacji i dystrybucji oprogramowania otwartoźródłowego to: GNU General Public Licence (GNU GPL)[21], MIT License[22] oraz Apache License[23]. Cechują się one wymogiem zachowania informacji o autorze i licencji, zaś pośród zasadniczych różnic wymienić można swobodę dotyczącą dalszego udostepniania zmian oprogramowania. Takie zasady licencjonowania za wykorzystywanie danego produktu są szczególnie przydatne dla użytkowników w ramach administracji państwowej oraz mikro, małych i średnich przedsiębiorstw, które ze względu na swój zazwyczaj organiczony budżet nie mogą pozwolić sobie na zakup rozwiązania komercyjnego.

Usługi tworzone na podstawie standardów otwartej i przejrzystej architektury, w tym komunikacyjnej (np. poprzez interfejsy programistyczne o otwartych standardach – OpenAPI) umożliwiają szeroką integrację rozwiązań typu open-source między sobą, jak i również z usługami płatnymi, korporacyjnymi o zamkniętym kodzie źródłowym. Powyższe jest jednocześnie jednym z czynników dalszej siły napędowej - swoistego koła zamachowego - rozwoju usług otwartoźródłowych, które łącząc się ze sobą są w stanie tworzyć większe, bardziej rozbudowane i kompleksowe środowiska.

Dodatkowym plusem wskazanego rozwiązania jest zaangażowanie społeczności do utrzymywania i ciągłego rozwoju systemu przez rozmaitych wolontariuszy, nie zaś przez pracowników korporacyjnych. Sprawia to, iż nie rzadko projekty open-source potrafią być bardziej innowacyjne i wychodzące naprzeciw oczekiwaniom użytkowników oczekujących nowych rozwiązań, jak

[18] 2024 Global Spotlight…, s. 6.
[19] M. Draouil, The End of Windows’: How France’s GendBuntu Signals a Shift from Costly, Patch-Plagued Systems, Medium 2025, https://medium.com/@majdidraouil/the-end-of-windows-how-france-s-gendbuntu-signals-a-shift-from-costly-patch-plagued-systems-2086aee86fe9 [dostęp: 29.11.2025].
[20] A. Żurek, Unia Europejska chce mieć własny system operacyjny. Nazywa się EU OS, Spidersweb 2025, https://spidersweb.pl/2025/03/unia-europejska-chce-miec-wlasny-system-operacyjny-to-pstryczek-w-strone-microsoftu.html [dostęp: 29.11.2025].
[21] Treść licencji GNU General Public Licence, Free Software Foundation, https://www.gnu.org /licenses/gpl-3.0.html. [dostep: 25.11.2025].
[22] Treść licencji MIT License, Massachusetts Institute of Technology, https://mit-license.org/. [dostęp: 25.11.2025].
[23] Treść licencji Apache License, https://www.apache.org/licenses/LICENSE-2.0.html. [dostęp: 25.11.2025].

i również umożliwiają „nieograniczone” wsparcie dla wykorzystywanego systemu. Powyższe stanowi często przeciwieństwo podejścia biznesowego, gdzie określone oprogramowanie rozwijane jest zazwyczaj przez określony czas, po czym wdrażane są jego inne odmiany lub zastępstwa – posiadające inne licencje, wymagania czy opłaty. W przypadku społeczności wolontariuszy system pozostaje serwisowany do momentu, aż dana społeczność bądź indywidualni utrzymujący nie uznają, iż należy zakończyć rozwój i/lub utrzymanie takowego projektu.

Wady wolnego oprogramowania

Jedną z największych wad wzmiankowanego oprogramowania jest jednocześnie jedną z największych zalet - przejrzystość i audytowalność kodu przez dowolną osobę, w tym osoby, które mogą być potencjalnymi adwersarzami. Przeglądanie kodu aplikacji można przecież czynić na potrzeby znalezienia w nim występujących podatności, celem późniejszej sprzedaży tej informacji na czarnym rynku, w tym np. do grup cyberofensywnych i cyberprzestępczych. Istnieje również możliwość, iż osoba, która natrafiła na lukę bezpieczeństwa w kodzie aplikacji zechce sama ją wykorzystać, aby osiągnąć własne cele bądź korzyści. Działanie takie jednak jest praktycznie nie możliwe w przypadku oprogramowania cechującego się zamkniętym kodem źródłowym (z wyłączeniem komercyjnych programów typu bug-bounty dających wybranym użytkownikom dostęp do fragmentów bądź całości kodu). Sprawia to, iż podmiot wykorzystujący otwartoźródłowe oprogramowanie musi zawsze mieć na uwadze m.in. zagrożenia wynikające ze złośliwych aktualizacji ogólnodostępnego kodu.

Poniekąd przykładem takiego działania była kompromitacja łańcucha dostaw oprogramowania npm, które stanowi największe na świecie repozytorium kodu JavaScript (npmjs.com). W 2025 roku amerykańska agencja ds. cyberbezpieczeństwa (ang. Cybersecurity & Infrastructure Security Agency, CISA) wydała ostrzeżenie odnośnie kompromistacji za pośrednictwem samoreplukującego się robaka o nazwie Shai-Hulud ponad 500 paczek npm[24]. Wskazane zagrożenie zmaterializowało się za pośrednictwem zainfekowanego komputera jednego z deweloperów, poprzez który adwersarz uzyskał dostęp do rejestru i opublikował w nim złośliwe paczki, które użytkownicy pobierali jednocześnie infekując swojej systemy. Komercyjne rozwiązania mają zazwyczaj rozbudowany system testowania wszelkich zmian w kodzie, który pomaga zniwelować takie zagrożenia; zaś w przypadku oprogramowania otwartoźródłowego nierzadko różni użytkownicy proponują swoje poprawki kodu zawierające złośliwe elementy deweloperom-wolontariuszom odpowiedzialnym za dany projekt.

Następną ważną kwestią wykorzystywania w organizacjach oprogramowania otwartoźródłowego jest zwyczajowy brak wsparcia producenta, którym są niejako (zwyczajowo) wolontariusze utrzymujący i rozwijający dany projekt. Sprawia to, iż jeśli podmiot decyduje się na produkcyjne wdrożenie u siebie rozwiązania otwartoźródłowego to musi mieć na uwadze, iż prawdopodobnie będzie zmuszona wdrażać je do swojej infrastruktury

[24] Widespread Supply Chain Compromise Impacting npm Ecosystem, CISA 2025, https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem [dostęp: 26.11.2025].

samodzielnie bez możliwości zlecenia pracy zewnętrznym konsultantom przy wdrażaniu aplikacji. Organizacja taka musi zakładać, iż podobnie jak i z wdrożeniem będzie na etapie utrzymania produktu we własnej infrastrukturze, gdzie to pracownicy danej organizacji będą ograniczeni do zapewnienia funkcjonowania usługi open-source za pomocą swoich zdolności, bądź ewentualnie z wykorzystaniem pomocy społeczności rozwijającej dane oprogramowanie. Alternatywą do wysokich kosztów zatrudnianai osób odpowiedzialnych za bieżące utrzymanie wskazanych systemów w ramach organizacji może być zakontrakotwanie firmy potrafiącej serwisować dany system w razie konieczności, co w przypadku oprogramowań otwartoźródłowych nie jest częste na rynku.

Kolejnym z opisywanych zagrożeń wykorzystywania oprogramowania otwartoźródłowego mogą być z czasem zmiany warunków świadczenia usług, udostępniania aplikacji bądź możliwości jej użytkowania i przejścia na inny model, np. z wolontariackiego na w pełni korporacyjny (biznesowy). Stosunkowo niedawnym przykładem zmiany modelu działania z oprogramowania niemal w pełni określanego jako FOSS, na niemal niwelowanie modelu bezpłatnego i faworyzwanie subskrybcji była popularna otwartoźródłowa platforma The Hive, służąca do prowadzenia śledztw z zakresu cyberbezpieczeństwa. Przedstawiciele tejże platformy zmienili w 2025 r. zasady licencjonowania i wykorzystywania produktu na bardziej restrykcyjne[25]. Powyższe mogło spowodować, iż dotychczasowi użytkownicy musieli zrezygonować z użytkowanego jak dotąd oprogramowania i szukać rozmaitych alternatyw.

Jako ostatnie z zagrożeń należy wskazać wykorzystywanie przez organizację mniejszych, mniej popularnych projektów open-source, co wiązać się może z istotnym ryzykiem związanym z możliwością porzucenia rozwoju i utraty wsparcia technicznego tych rozwiązań ze strony deweloperów-wolontariuszy projektów. Przedsięwzięcia takie mogą nie dysponować wystarczającą liczbą aktywnych deweloperów ani stabilnym zapleczem społecznościowym, co może prowadzić od ich szybkiego zaniku i braku aktualizacji. W efekcie organizacja może zostać pozostawiona bez dostępu do poprawek bezpieczeństwa oraz aktualizacji kompatybilności, co tym samym zwiększa podatność na możliwe awarie i zagrożenia bezpieczeństwa teleinformatycznego. Ponadto trudności trudności z wdrażaniem mniejszych, mniej popularnych projektów pojawiają się przy integracji z innymi systemami, a organiczona dokumentacja dodatkowo komplikuje obsługę i dalszy rozwój oprogramowania.

Znaczenie oprogramowania otwartoźródłowego dla podmiotów administracji publicznej i środowisk biznesowych

Organy administracji państwowej są systematycznie niedofinansowane, co sprawia, iż muszą one ograniczać swoje wydatki na rozmaite sposoby[26]. Jednym z takowych sposobów jest minimalizacja kosztów pod kątem wykorzystywanych oraz planowanych usług z zakresu teleinformatyki i cyberbezpieczeństwa. Podobna sytuacja konieczności prorytetyzacji raczej

[25] Informacje o licencji produktu The Hive, StrangeBee, https://docs.strangebee.com /thehive/installation/licenses/license/ [dostęp: 26.11.2025].
[26] Zadłużenie Sektora Finansów Publicznych II kw. 2025. Biuletyn kwartalny, Ministerstwo Finansów 2025, s. 1.

skromnych budżetów występować może w mikro, małych i średnich przedsiębiorstwach, które ze względu na swój ograniczony budżet muszą bacznie pilnować wszelkich wydatków.

Powyższe sprawia, iż podmioty te nie rzadko nie mogą sobie pozwolić na pewne rozwiązania teleinformatyczne i zmuszone są niejako posiłkować się zamiennikami, bądź próbować radzić sobie bez takowych narzędzi. Idealnym remedium na zastany stan rzeczy są rozwiązania otwartoźródłowe tworzone jako alternatywy dla najpopularniejszych rozwiązań komercyjnych, takich jak: Microsoft Office, systemy operacyjne (Microsoft Windows, MacOS), liczne rozwiązania chmurowe (AWS, Azure), czy systemy korelacji informacji i zdarzeń w środowiskach teleinformatycznych podmiotów (ang. Security Information and Event Management, SIEM). Dzięki zastosowaniu sprawdzonych i dojrzałych narzędzi otwartoźródłowych podmioty te są w stanie uniknąć wysokich kosztów związanych z utrzymaniem, czy licencjonowaniem produktów komercyjnych. Należy jednak pamiętać, iż znaczna część rozwiązań biznesowych w różnym stopniu opiera się na rozwiązaniach otwartoźródłowych jako podwalinach swoich narzędzi sprzedawanych komercyjnie, stąd organizacje często mogą nie zdawać sobie sprawy, iż oprogramowania *open-source* już funkcjonują w ich infrastrukturze teleinformatycznej.

Dodatkowo podmioty kluczowe z punktu widzenia bezpieczeństwa państwa takiej jak urzędy administracji centralnej, służby specjalne, Siły Zbrojne RP, czy operatorzy infrastruktury krytycznej stosując oprogramowanie otwartoźródłowe mają możliwość częściowego lub całkowitego uniezależnienia się od zagranicznych rozwiązań technologicznych celem osiągnięcia większej suwerenności cyfrowej. Podejście takie wymaga jednak wieloetapowego planu tranzycji i konsekwencji decyzyjnej obranej ścieżki. Jeśli podmiot zdecydowałby się na przykładowe przejście na technologie otwartoźródłowe w wymiarze całkowitym (od aplikacji przeznaczonej dla użytkownika końcowego, po systemy operacyjne i rozwiązania administracyjno-serwerowe) należałoby opracować wieloetapowy plan przejścia na takowe rozwiązania oraz utrzymywania budowanych zdolności przez następne lata.

Nie można jednocześnie zapominać o zagrożeniach wynikających z stosowania orpogramowania opracowwyanego przez deweloperów-wolontariuszy, a nie komercyjną firmę gwarantującą niejako bezpieczeństwo kodu swoją marką i reputacją. Przedstawione wcześniej przykłady zagrożeń ukazują jak istotne z punktu widzenia organizacji są wielowarstwowe zabezpieczenia, które pozwolą uchronić podmiot pod kątem ewentualnego uruchomienia we własnym środowisku niebezpiecznej lub wprost złośliwej aplikacji. Jednym z podstawowych zabezpieczeń organizacyjnych przed tego przykładowym atakiem na łańcuch dostaw kolejnych wersji aplikacji może być zastosowanie tzw. modelu zabezpieczeń „*Zero trust”* (zerowego zaufania), jako jednego z filarów współczesnego bezpieczeństwa teleinfromatycznego organizacji[27].

[27] G. Pilarski, Podejście „Zero Trust” w obszarze bezpieczeństwa informacyjnego, „Rocznik Bezpieczeństwa Morskiego” 2024, Tom: XVIII, s. 315 i n.

Podsumowanie

Oprogramowanie otwartoźródłowe stanowi strategiczną alternatywę dla rozwiązań korporacyjnych, oferując kluczowe zalety, takie jak brak kosztów licencyjnych, elastyczność modyfikacji kodu źródłowego oraz szybkie aktualizacje bezpieczeństwa dzięki globalnej społeczności deweloperów i entuzjastów. Transparentność kodu eliminuje ryzyko ukrytych funkcji typu „backdoor" czy „kill-switch", co jest szczególnie istotne dla administracji państwowej, gdzie niedofinansowanie budżetów wymusza efektywne, niezależne od vendorów rozwiązania, oraz dla mikro, małych i średnich przedsiębiorstw szukających niskokosztowych wdrożeń bez konieczności zamknięcia się na jednego dostawcę oprogramowania (vendor lock-in). Jednocześnie wady oprogramowania open-source, takie jak brak gwarantowanego wsparcia technicznego, potrzeba wewnętrznych kompetencji IT i potencjalne ryzyka w niszowych projektach z wolniejszym tempem aktualizacji, wymagają świadomego zarządzania – np. poprzez wybór popularnych dystrybucji z komercyjnym wsparciem lub audyty społecznościowe. W kontekście administracji państwowej oraz operatorów infrastruktury krytycznej, oprogramowanie otwartoźródłowe wspiera suwerenność cyfrową, minimalizując zależności geopolityczne (np. od dostawców wysokiego ryzyka), podczas gdy dla przedsiębiorstw zapewnia skalowalność i innowacyjność bez barier finansowych. Ostatecznie, przewaga społecznościowej innowacji i przejrzystości czyni aplikacje otwartoźródłowe optymalnym wyborem dla organizacji priorytetyzujących długoterminową niezależność i oszczędności, pod warunkiem dysponowania zasobami ludzkimi oraz konsekwentnej realizacji odpowiedniej strategii wdrożeniowej.

Po przeprowadzonej identyfikacji wad i zalet oprogramowania otwartoźródłowego należy rozważyć możliwość przeprowadzenia badań nad implementacją danych narzędzi w wybranych organizacjach (np. administracji państwowej) celem określenia możliwych sposobów ich praktycznego wdrożenia oraz zmian technologicznych i organizacyjnych z tego wynikających.

Bibliografia

Barcikowski W., Wykorzystanie otwartego oprogramowania w informatycznych systemach zarządzania, „Nowoczesne systemy zarządzania" 2012.

Browser Market Share Report for 2025 Q3, Cloudflare 2025, https://radar.cloudflare.com/reports/browser-market-share-2025-q3.

Chesbrough H., Measuring the Economi Value of Open Source, The Linux Foundation 2023.

Draouil M., The End of Windows': How France's GendBuntu Signals a Shift from Costly, Patch-Plagued Systems, Medium 2025, https://medium.com/@majdidraouil/the-end-of-windows-how-france-s-gendbuntu-signals-a-shift-from-costly-patch-plagued-systems-2086aee86fe9.

Gómez A., Muñoz A., Deep Learning-Based Attack Detection and Classification in Android Devices, "Electronics" 2023 (12).

Korac S. i in., Ransomware: Analysis and Evaluation of Live Forensic Techniques and the Impact on Linux based IoT Systems [w:] 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Edinburgh Napier University 2024.

Makowiec P., Przełomowa decyzja niemieckiego landu. „Chcemy cyfrowej niezależności", CyberDefence24 2024, https://cyberdefence24.pl/cyberbezpieczenstwo/przelomowa-decyzja-niemieckiego-landu-chcemy-cyfrowej-niezaleznosci.

Pancevski B., U.S. Officials Say Huawei Can Covertly Access Telecom Networks, The Wall Street Journal 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

Pantak A., Czy Polskę czeka spór z Huawei? Chodzi o projekt nowych przepisów o cyberbezpieczeństwie, Gazeta Prawna 2025, https://www.gazetaprawna.pl/firma-i-prawo/artykuly/10562128,czy-polske-czeka-spor-z-huawei-chodzi-o-projekt-nowych-przepisow-o-cy.html.

Pilarski G., Podejście „Zero Trust" w obszarze bezpieczeństwa informacyjnego, „Rocznik Bezpieczeństwa Morskiego" 2024, Tom: XVIII.

Pilarski G., Przegląd współczesnych zagrożeń w cyberprzestrzeni, „Problemy Techniki Uzbrojenia" 2023, t. 167, nr 5.

Pollet M., European Commission backlists groups lobbying for Huawei, Politico 2025, https://www.politico.eu/article/european-commission-blacklists-lobby-groups-tied-to-huawei/.

Sesterhenn E., Schneeweisz J., Vervier M., Source Code Audit on Git for Open Source Technology Improvement Fund (OSTIF), X41 D-SEC 2025.

Zeeuw A. i in., The orchestrated digital inequalities of the IoT: How vendor lock-in hinders and playfulness creates IoT benefits in every life, "New Media & Society" 2024, vol. 26, issue 10.

Żurek A., Unia Europejska chce mieć własny system operacyjny. Nazywa się EU OS, Spidersweb 2025, https://spidersweb.pl/2025/03/unia-europejska-chce-miec-wlasny-system-operacyjny-to-pstryczek-w-strone-microsoftu.html.