

WOJSKOWA AKADEMIA TECHNICZNA

im. Jarosława Dąbrowskiego

WYDZIAŁ CYBERNETYKI



**Temat pracy: REKONESANS WZGLĘDEM DOMENY
INTEGRACJE-AMBIENTE.PL**

KRYPTOLOGIA I CYBERBEZPIECZEŃSTWO

(kierunek studiów)

CYBEROBRONA

(specjalność)

Autor:

Łukasz ROZBICKI

Warszawa 2025

Spis treści

Rozdział I Uzasadnienie wyboru domeny	4
Rozdział II Dane ogólne dotyczące organizacji będącej właścicielem domeny	5
II.1. Informacje ogólne o organizacji.....	5
II.2. Dane rejestrowe i finansowe	7
II.3. Dane kontaktowe i lokalizacja	9
II.4. Podsumowanie	10
Rozdział III Serwery DNS obsługujące domenę	11
III.1. Nazwy i adresy IP serwerów.....	11
III.2. Zabezpieczenia.....	15
III.3. Podsumowanie	16
Rozdział IV Ogólne dane dotyczące witryny domeny	17
IV.1. Dane statystyczne dotyczące popularności i rankingów	17
IV.2. Intensywność modyfikacji strony	22
IV.3. Usługi świadczone dla klientów	25
IV.4. Podsumowanie	28
Rozdział V Struktura domeny	29
V.1. Poddomeny	29
V.2. Komputery w domenie i poddomenach.....	31
V.3. diagramy struktury domeny	32
V.4. Podsumowanie	34
Rozdział VI Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi	35
VI.1. Systemy operacyjne:	35
VI.2. Usługi sieciowe.....	36
VI.3. Aplikacje realizujące usługi sieciowe:	38
VI.4. Podsumowanie	39
Rozdział VII Wykorzystywane technologie informatyczne	40

VII.1. Wykorzystywane technologie informatyczne.....	40
VII.2. Podsumowanie.....	43
Rozdział VIII Pracownicy i osoby powiązane	44
VIII.1. Uzyskane informacje dotyczące pracowników organizacji	44
VIII.2. Podsumowanie	49
Rozdział IX Bezpieczeństwo.....	50
IX.1. Stwierdzone podatności.....	50
IX.2. Złośliwe oprogramowanie	57
IX.3. Zagrożenia dla innych	60
IX.4. Stosowane mechanizmy ochronne	61
IX.5. Podsumowanie	63
Rozdział X Stosowane urządzenia sieciowe	64
X.1. Infrastruktura sieciowa	64
X.2. Podsumowanie	67
Rozdział XI Podsumowanie	68

Rozdział I Uzasadnienie wyboru domeny

Domena integracje-ambiente.pl została wybrana ze względu na jej związek z branżą organizacji wydarzeń integracyjnych, co pozwala na analizę zróżnicowanych aspektów infrastruktury sieciowej i zabezpieczeń. Strona reprezentuje firmę działającą na rynku lokalnym, co daje możliwość zbadania struktury technicznej i zastosowanych technologii w kontekście regionalnym. Charakter domeny, związany z dynamiczną branżą usługową, czyni ją interesującym obiektem analizy, szczególnie pod kątem bezpieczeństwa, wydajności oraz zgodności z nowoczesnymi standardami sieciowymi. Wybór ten umożliwia również ocenę wdrożonych rozwiązań technicznych w kontekście ich skuteczności i potencjalnych obszarów do optymalizacji.

Rozdział II Dane ogólne dotyczące organizacji będącej właścicielem domeny

II.1. Informacje ogólne o organizacji

ZAPRASZAMY DO ZAPOZNANIA SIĘ Z NASZĄ OFERTĄ!

- Specjalizujemy się w organizacji imprez plenerowych oraz imprez tematycznych dla grup w całej Polsce.
- W województwie mazowieckim dysponujemy terenem o powierzchni ponad 50 ha w okolicach Radziejowic - zróżnicowanym pod względem ukształtowania terenu - idealnym do off-road'u, na którym można jeździć legalnie!
- Organizujemy imprezy dla małych grup oraz bardzo dużych zapewniając każdemu odpowiednią porcję rozrywki i wrażeń
- Współpracujemy z kilkoma hotelami w okolicy oraz wieloma hotelami w całej Polsce, gdzie zapewniamy naszym Klientom najlepsze warunki organizowania konferencji i noclegów oraz przeprowadzenia zajęć team-building
- W plenerze polecamy imprezy:
 - off-road: quady, samochody terenowe, amfibie, skutery śnieżne
 - survival,
 - gry militarne
 - gry terenowe tematyczne
 - konkurencje alpinistyczne i zabawy sprawnościowe
 - paintball i paintball militarny
 - sporty wodne (w zależności od lokalizacji): spływy kajakowe, skutery wodne, windsurfing, nurkowanie, wave-boarding
 - eksploracja jaskiń
 - loty helikopterem, skoki spadochronowe, loty szybowcem
 - gry miejskie
 - Zapewniamy zadaszenie, ognisko i catering – możemy dopasować zakres do potrzeb Klienta.
- W naszej ofercie znajdziecie bogatą ofertę na wieczór:
 - biesiady tematyczne
 - gry i zabawy fabularne na terenie hotelu
 - degustacje, pokazy barmańskie
 - wieczory z tańcem w roli głównej (w połączeniu z nauką tańca)
 - liczne warsztaty kulinarne i artystyczne
- Działamy w całej Polsce, zarówno przy organizacji wybranych zajęć team-building jak i kompleksowo organizując cały wyjazd – zgodnie z życzeniem Klienta. Współpracujemy z wieloma obiektami o różnym standardzie zapewniając naszym Klientom atrakcyjne warunki.
- Dysponujemy terenem o powierzchni ponad 40 ha w okolicach Radziejowic-zróżnicowanym pod względem ukształtowania terenu i idealnym do off-road'u, z nowo powstałym torzem szkoleniowym off-road i zadaszonymi wiatami mogącymi pomieścić około 180 osób. Teren jest odpowiedni również do organizacji pikników.
- Przy imprezach plenerowych zapewniamy zadaszenie, ognisko, catering- możemy dopasować zakres do potrzeb Klienta.
- Nasz zespół to profesjonalisi w swoich dziedzinach i pasjonaci. Zespół, który się zna ze sobą nawzajem, zna powierzone zadania i posiada wieloletnie doświadczenie w realizacji wybranych zajęć team-building.
- Posiadamy własny sprzęt, instruktorów, animatorów, autorskie scenariusze, dekoracje oraz własny teren do organizacji imprez.
- Każdy scenariusz jest indywidualnie dopasowany do potrzeb Klienta, wielkości grupy i miejsca, gdzie integracja jest realizowana.

Obraz 1. integracje-ambiente.pl zakładka o-nas

DATY ZWIĄZANE Z DZIAŁALNOŚCIĄ PODMIOTU

data wpisu do rejestru lub ewidencji 2011-12-05

data skreślenia z rejestru lub ewidencji

data powstania 1992-06-11

data rozpoczęcia działalności 1992-06-11

data wpisu do REGON

data zawieszenia działalności

data wznowienia działalności 2022-04-05

data zakończenia działalności

data skreślenia z REGON

data orzeczenia o ogłoszeniu upadłości

data zakończenia postępowania upadłościowego

Obraz 2. (stat.gov.pl)

Powyższe obrazy (Obraz 1. i 2.) dostarczają informacje na temat:

1) Zakres działania:

- Organizacji imprez plenerowych i tematycznych na terenie całej Polski – zarówno dla grup małych, jak i dużych.
- Realizacji imprez integracyjnych typu off-road (quady, samochody terenowe, amfibie), gier terenowych oraz aktywności survivalowych.
- Współpracy z hotelami (m.in. w okolicach Radziejowic i w innych rejonach Polski), co pozwala na organizację konferencji, noclegów i różnego rodzaju spotkań integracyjnych.
- Zapewnianiu atrakcji wieczornych (biesiady tematyczne, gry fabularne w hotelu, pokazy barmańskie, warsztaty kulinarne, etc.).
- Kompleksowej obsłudze eventów (zapewnienie miejsca, animacji, nagłośnienia i w razie potrzeby – także cateringu i innych usług towarzyszących).

2) Historia organizacji:

- a) Data powstania (1992-06-11) – sugeruje, że początki działalności sięgają lat 90.
- b) Data wpisu do rejestru lub ewidencji (2011-12-05) – wskazuje na formalne zarejestrowanie przedsiębiorstwa (lub kolejnej formy prowadzonej działalności) w odpowiednim rejestrze gospodarczym w roku 2011.
- c) Data wznowienia działalności (2022-04-05) – sugeruje przerwę i ponowne podjęcie aktywności gospodarczej (możliwe, że działalność była zawieszona i reaktywowano ją w 2022 roku).
- d) Brak wpisów na temat ogłoszenia upadłości czy zakończenia postępowania upadłościowego – co oznacza, że firma wedle publicznych rejestrów nie była objęta formalnym postępowaniem upadłościowym.

II.2. Dane rejestrowe i finansowe

Dane Rejestrowe

NAZWA PEŁNA	ADRES DO DORECZEŃ
"AMBIENTE INTEGRACJE" MARZENA TOMASIK	ul. Dębowa 20, 96-323 Dębiny Osuchowskie
	Pokaż na mapie
NIP	5341582023
REGON	014963466
Forma prawna	indywidualna działalność gospodarcza
Adres rejestrowy	ul. Dębowa 20, 96-323 Dębiny Osuchowskie
Przedsiębiorca	MARZENA TOMASIK
Data rozpoczęcia działalności w CEIDG	1992-06-11
Zobacz więcej	
KODY PKD	
93.29.B - Pozostała działalność rozrywkowa i rekreacyjna	
Zobacz więcej	
STATUS PODATNIKA VAT	
CZYNNY	
NUMERY RACHUNKÓW BANKOWYCH Z REJESTRU VAT	
PL11 1050 1025 1000 0090 6830 5433 PL26 1050 1025 1000 0090 6134 9487	

Obraz 3.(aleo.com)

Figuruje w rejestrze VAT	
Firma (nazwa) lub imię i nazwisko	MARZENA TOMASIK
Numer, za pomocą którego podmiot został zidentyfikowany na potrzeby podatku, jeżeli taki numer został przyznany	5341582023
Status podatnika (wg stanu na dzień sprawdzenia 17-01-2025)	Czynny
Numer identyfikacyjny REGON, o ile został nadany	014963466
Numer w Krajowym Rejestrze Sądowym, o ile został nadany	-
Adres siedziby – w przypadku podmiotu niebędącego osobą fizyczną	-
Adres stałego miejsca prowadzenia działalności albo adres miejsca zamieszkania, w przypadku braku adresu stałego miejsca prowadzenia działalności - w odniesieniu do osoby fizycznej	DĘBOWA 20, 96-320 DĘBINY OSUCHOWSKIE
Imiona i nazwiska prokurentów oraz ich numery identyfikacji podatkowej	-
Imiona i nazwiska osób wchodzących w skład organu uprawnionego do reprezentowania podmiotu oraz ich numery identyfikacji podatkowej	-
Imię i nazwisko lub firma (nazwa) wspólnika oraz jego numer identyfikacji podatkowej	-
Numery rachunków rozliczeniowych lub imiennych rachunków w SKOK	11 1050 1025 1000 0090 6830 5433 26 1050 1025 1000 0090 6134 9487
Data rejestracji jako podatnika VAT	1999-05-31

Obraz 4. (www.podatki.gov.pl)

Powyższe obrazy (Obraz 3. i 4.) dostarczają informacje na temat:

1) Nazwa przedsiębiorstwa i forma prawa:

- Nazwa: „AMBIENTE INTEGRACJE” MARZENA TOMASIK
- Forma prawa: indywidualna działalność gospodarcza
- Podmiot został zarejestrowany w CEIDG (Centralna Ewidencja i Informacja o Działalności Gospodarczej).

2) Identyfikatory rejestrowe:

- NIP: 5341582023
- REGON: 014963466
- Data rozpoczęcia działalności w CEIDG: 1992-06-11
- Status podatnika VAT: czynny (wg stanu na dzień widoczny w rejestrze).

3) Adres rejestrowy:

- ul. Dębowa 20, 96-323 Dębiny Osuchowskie
- Adres ten figuruje zarówno jako siedziba firmy, jak i adres doręczeń.

4) Numery rachunków bankowych (z rejestru VAT)

- PL11 1050 1025 1000 0090 6830 5433
- PL26 1050 1025 1000 0090 6134 9487
- Oba rachunki są zarejestrowane do rozliczeń podatkowych VAT, co oznacza, że mogą służyć do oficjalnych transakcji związanych z działalnością gospodarczą podmiotu.

5) Zakres PKD (kody działalności)

- Główny kod PKD to 93.29.B – „Pozostała działalność rozrywkowa i rekreacyjna”, co jest spójne z ofertą imprez integracyjnych i eventów plenerowych prezentowanych przez firmę.

II.3. Dane kontaktowe i lokalizacja

Kontakt

Ambiente Marzena Tomaszik
Budy Michałowskie 72, 96-316 Miedzyborów

Email: marzena@integracje-ambiente.pl Mobile: +48 695 351 513
marzena@imprezy-integracyjne-ambiente.pl

Obraz 5. integracje-ambiente.pl strona główna

DZIAŁALNOŚĆ GOSPODARCZA PODLEGAJĄCA WPISOWI DO CEIDG

INFORMACJE PODSTAWOWE	
nazwa	"AMBIENTE INTEGRACJE" MARZENA TOMASIK
organ rejestrowy	MINISTER ROZWOJU, PRACY I TECHNOLOGII
rodzaj rejestru lub ewidencji	CENTRALNA EWIDENCJA I INFORMACJA O DZIAŁALNOŚCI GOSPODARCZEJ
numer w rejestrze ewidencji	
ADRES SIEDZIBY	
kraj	POLSKA
województwo	MAZOWIECKIE
powiat	żyrardowski
gmina	Mszczonów
miejscowość	Dębiny Osuchowskie
ulica	ul. Dębowa
nr nieruchomości	20
nr lokalu	
kod pocztowy	96-323
nietypiczne miejsce lokalizacji	

Obraz 6. prod.ceidg.gov.pl

Powyższe obrazy (Obraz 3. i 4.) dostarczają informacje na temat:

1) Dane kontaktowe

- Nazwa firmy: „AMBIENTE INTEGRACJE” Marzena Tomaszik
- Adres: Budy Michałowskie 72, 96-316 Miedzyborów
- Email:
 - marzena@integracje-ambiente.pl
 - marzena@imprezy-integracyjne-ambiente.pl
- Telefon: +48 695 351 513

2) Lokalizacja

- Kraj: Polska
- Województwo: Mazowieckie
- Powiat: Żyrardowski
- Gmina: Mszczonów

- Miejscowość: Dębiny Osuchowskie
- Ulica: ul. Dębowa
- Nr nieruchomości: 20
- Kod pocztowy: 96-323

II.4. Podsumowanie

W rozdziale II przedstawiono kompleksowe informacje dotyczące podmiotu będącego właścicielem domeny integracje-ambiente.pl. Zidentyfikowano przedsiębiorstwo „AMBIENTE INTEGRACJE” MARZENA TOMASIK, prowadzące indywidualną działalność gospodarczą w oparciu o wpis w CEIDG oraz figurujące jako czynny podatnik VAT. Analiza danych rejestrowych potwierdziła długą historię funkcjonowania firmy (od 1992 roku) i ujawniła kluczowe numery identyfikacyjne (NIP, REGON), a także dwa rachunki bankowe związane z rozliczeniami podatkowymi.

Dodatkowo ustalono adresy korespondencyjne, w tym oficjalną siedzibę w Dębinach Osuchowskich oraz drugi adres podawany w materiałach kontaktowych (Budy Michałowskie). Zaprezentowane dane kontaktowe (adresy e-mail w domenie integracje-ambiente.pl i numer telefonu) wskazują na jawne i aktywne formy komunikacji z przedsiębiorstwem. Wszystkie te informacje tworzą spójny obraz firmy specjalizującej się w organizacji imprez integracyjnych, co koresponduje z wcześniejszymi ustaleniami dotyczącymi zakresu działalności

Z uwagi na formę prawną działalności, nie uzyskano danych finansowych. Nie odnaleziono również regulaminów ani informacji o partnerach biznesowych związanych z organizacją.

Rozdział III Serwery DNS obsługujące domenę

III.1. Nazwy i adresy IP serwerów

Nazwa domeny	integracje-ambiente.pl
Stan	Aktywna w DNS [REGISTERED]
Utworzona	2019.08.22 15:22:54
Ostatnia modyfikacja	2024.07.25 11:04:03
Koniec okresu rozliczeniowego	2025.08.22 15:22:54
Nazwy serwerów	ns1.3wdt.pl [195.246.126.114] ns2.3wdt.pl [195.246.126.115]
Abonent	Ambiente Marzena Tomasik Budy Michałowskie 72 96-316 Międzyborów, pl +48.695351513 Typ abonenta: organizacja Ostatnia modyfikacja: 2018.09.10 12:42:39
Rejestrator	Digital Media Technology Sp. z o.o. ul. Grunwaldzka 15/4 31-524 Kraków tel: +48.517180045 https://dmtec.pl/kontakt

Obraz 7. Wynik wyszukiwania domeny na stronie www.dns.pl

Whois Record (last updated on 2025-01-18)

DOMAIN NAME:	integracje-ambiente.pl
registrant type:	organization
nameservers:	ns1.3wdt.pl. [195.246.126.114] ns2.3wdt.pl. [195.246.126.115]
created:	2019.08.22 15:22:54
last modified:	2024.07.25 11:04:03
renewal date:	2025.08.22 15:22:54
no option	
dnssec:	Unsigned
REGISTRAR:	
Digital Media Technology Sp. z o.o.	
ul. Grunwaldzka 15/4	
31-524 Kraków	
tel: +48.517180045	
https://dmtec.pl/kontakt	
WHOIS database responses:	https://dns.pl/en/whois

Obraz 8. Wynik wyszukiwania domeny na stronie [whois.domaintools.com](https://whois.domaintools.com/integracje-ambiente.pl)

Na podstawie danych z rejestru WHOIS oraz analizy dns (Obraz 7. i Obraz 8.) ustalono, że domena integracje-ambiente.pl korzysta z następujących serwerów nazw:

ns1.3wdt.pl – adres IP: 195.246.126.114

ns2.3wdt.pl – adres IP: 195.246.126.115

Result for: INTEGRACJE-AMBIENTE.PL

Contract All ▲ Download Records

Jump to: A Records AAAA Records CNAME Records MX Records NS Records PTR Records SRV Records SOA Records TXT Records CAA Records DS Records DNSKEY Records

A [SHOW RAW]

Type	Domain Name	TTL	Address
A	integracje-ambiente.pl	14400	195.246.126.117 Owner: Domena.pl Sp. z o.o. WHOIS AS60713

AAAA

CNAME

MX [SHOW RAW]

Type	Domain Name	TTL	Preference	Address
MX	integracje-ambiente.pl	14400	0	integracje-ambiente.pl.(195.246.126.117 Owner: Domena.pl Sp. z o.o. WHOIS AS60713)

NS [SHOW RAW]

Type	Domain Name	TTL	Canonical Name
NS	integracje-ambiente.pl	21600	ns2.3wdt.pl. (195.246.126.116 Owner: Domena.pl Sp. z o.o. WHOIS AS60713)
NS	integracje-ambiente.pl	21600	ns1.3wdt.pl. (195.246.126.114 Owner: Domena.pl Sp. z o.o. WHOIS AS60713)

Obraz 9. Wynik wyszukiwania domeny na stronie dnschecker.org

DNS Records

Domain Records PTR Records

NS Records	IP	Provider	ASN
ns2.3wdt.pl used by 86 domains	195.246.126.116 (PL)	EXEA Sp. z o.o. (PL)	60713
ns1.3wdt.pl used by 86 domains	195.246.126.114 (PL)	EXEA Sp. z o.o. (PL)	60713

A/AAAA Records	Provider	ASN
195.246.126.117 (PL) used by 74 domains	EXEA Sp. z o.o. (PL)	60713

MX Records	IP	Provider	ASN
integracje-ambiente.pl used by 1 domain	195.246.126.117 (PL)	EXEA Sp. z o.o. (PL)	60713

SPF record

```
v=spf1 ip4:195.246.126.117 +a +mx ~all
```

Obraz 10. Wynik wyszukiwania domeny na stronie search.dnslytics.com

Dodatkowe dane uzyskane z narzędzi do analizy DNS (Obraz 9. I Obraz 10.) potwierdzają i uzupełniają wcześniejsze informacje:

1) NS Records

- Domena integracje-ambiente.pl wskazuje te same serwery nazw:
 - ns1.3wdt.pl o IP 195.246.126.114
 - ns2.3wdt.pl o IP 195.246.126.116
- Z narzędzi DNS wynika, że obydwa serwery znajdują się w infrastrukturze firmy EXEA Sp. z o.o. (ASN 60713).

2) A oraz MX Records

- Główny rekord A dla integracje-ambiente.pl to 195.246.126.117, co wskazuje na adres serwera hostingowego odpowiadającego za stronę WWW.
- Ten sam adres widnieje w rekordzie MX, co oznacza, że poczta (e-mail) dla domeny jest obsługiwana prawdopodobnie na tym samym serwerze.

Rozbieżność w jednym z adresów IP serwera NS (195.246.126.115 vs. 195.246.126.116) może wynikać z dynamicznej konfiguracji usług DNS lub z przejściowego stanu informacji w różnych bazach. Kluczowe jest to, że oba serwery nazw należą do jednego dostawcy i działają w ramach tej samej puli adresowej (AS60713).

III.2. Zabezpieczenia

Analyzing DNSSEC problems for [integracje-ambiente.pl](#)

	<ul style="list-style-type: none"> ✓ Found 3 DNSKEY records for . ✓ DS=20326/SHA-256 verifies DNSKEY=20326/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
pl	<ul style="list-style-type: none"> ✓ Found 2 DS records for pl in the . zone ✓ DS=48559/SHA-256 has algorithm RSASHA256 ✓ DS=42290/SHA-256 has algorithm RSASHA256 ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=26470 and DNSKEY=26470 verifies the DS RRset ✓ Found 2 DNSKEY records for pl ✓ DS=42290/SHA-256 verifies DNSKEY=42290/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=42290 and DNSKEY=42290/SEP verifies the DNSKEY RRset
integracje-ambiente.pl	<ul style="list-style-type: none"> ✗ No DS records found for integracje-ambiente.pl in the pl zone ✗ No DNSKEY records found ✓ ns2.3wdt.pl is authoritative for integracje-ambiente.pl ✓ integracje-ambiente.pl A RR has value 195.246.126.117 ✗ No RRSIGs found
integracje-ambiente.pl	<ul style="list-style-type: none"> ✓ ns1.3wdt.pl is authoritative for integracje-ambiente.pl ✓ integracje-ambiente.pl A RR has value 195.246.126.117 ✗ No RRSIGs found

Obraz 11. Wynik wyszukiwania domeny na dnssec-analyzer.verisignlabs.com

Diagnostyka DNS (Obraz 11.) dla domeny integracje-ambiente.pl dostarczyła informacje na temat:

1) Brak wsparcia dla DNSSEC:

- Nie znaleziono wpisów DS (Delegation Signer) w strefie nadzędnej .pl, co oznacza, że ta domena nie jest „podpisana” w ramach łańcucha zaufania DNSSEC.
- Nie istnieją również rekordy DNSKEY i RRSIG, które są niezbędne do uwierzytelniania odpowiedzi DNS w modelu DNSSEC.

2) Serwery nazw:

- Serwery ns1.3wdt.pl i ns2.3wdt.pl działają poprawnie jako autorytywne, obsługując adres IP 195.246.126.117 dla domeny. Brak niezgodności w tej konfiguracji.

III.3. Podsumowanie

W rozdziale III dokonano analizy serwerów DNS obsługujących domenę integracje-ambiente.pl oraz sprawdzono zastosowane w niej mechanizmy zabezpieczające. Ustalono, że domena korzysta z dwóch serwerów nazw:

- ns1.3wdt.pl – zazwyczaj o adresie IP 195.246.126.114,
- ns2.3wdt.pl – widoczny w różnych narzędziach pod adresami 195.246.126.115 lub 195.246.126.116.

Różnica w adresie IP dla serwera ns2.3wdt.pl może wynikać m.in. z:

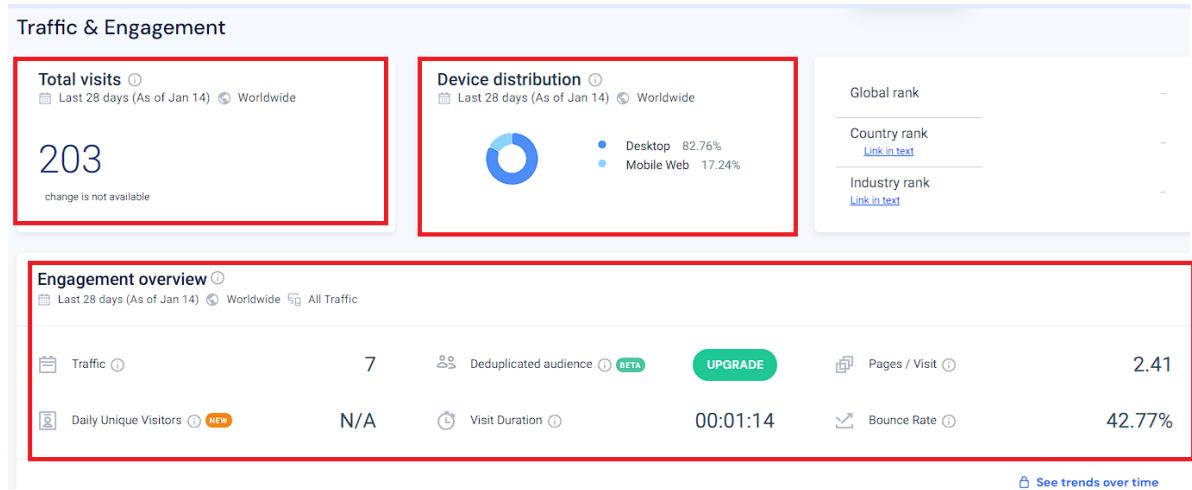
- Aktualizacji lub zmiennej konfiguracji (np. po zmianie adresu IP, niektóre bazy WHOIS lub narzędzia DNS mogą jeszcze przechowywać starszą wartość),
- Obecności kilku adresów przypisanych do jednego hosta (tzw. multi-homing) wówczas w zależności od serwera DNS lub narzędzia, może być zwracany inny adres IP,
- Mechanizmów równoważenia obciążenia (load balancing) bądź geolokalizacji serwera, gdzie host może mieć przypisanych kilka IP i dynamicznie je zmieniać.

Oba serwery działają w ramach tego samego autorytywnego systemu DNS i są zarządzane przez tego samego dostawcę hostingowego (3wdt.pl / EXEA). Analiza nie wykazała jednak wdrożenia protokołu DNSSEC – brak rekordów DS, DNSKEY oraz RRSIG wskazuje, że domena integracje-ambiente.pl nie korzysta z kryptograficznego zabezpieczenia odpowiedzi DNS.

Wnioskiem z przeprowadzonej analizy jest to, że domena jest poprawnie obsługiwana przez dwa serwery DNS, lecz brakuje w niej rozszerzonych środków bezpieczeństwa na poziomie DNS (DNSSEC)

Rozdział IV Ogólne dane dotyczące witryny domeny

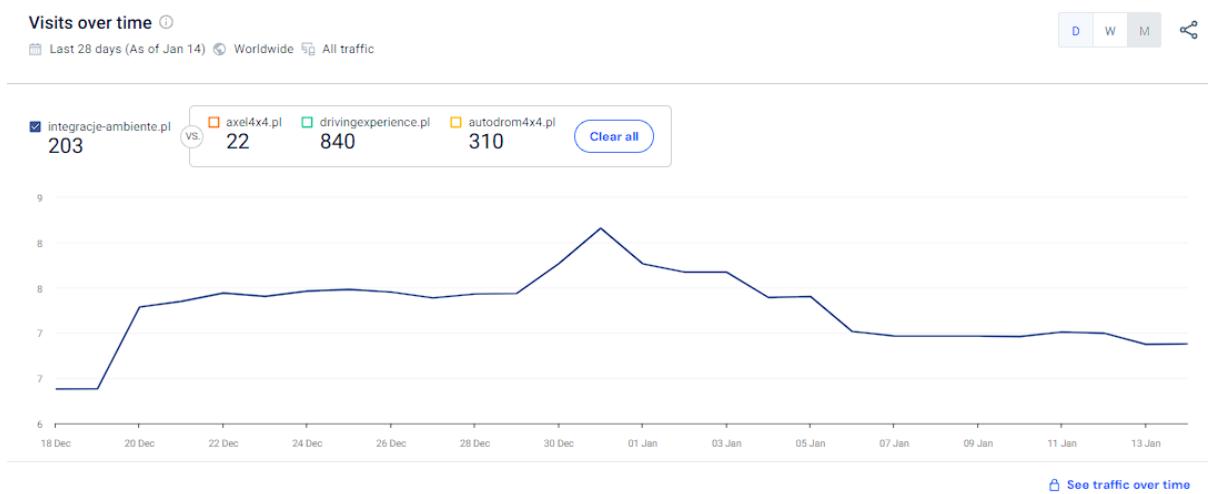
IV.1. Dane statystyczne dotyczące popularności i rankingów



Obraz 12. Wyniki wyszukiwania domeny na pro.similarweb.com

W celu oszacowania popularności serwisu integracje-ambiente.pl przeprowadzono analizę w narzędziu SimilarWeb (Obraz 12.) które przedstawia dane statystyczne związane z popularnością i rankingami witryny z okresu 18 grudnia 2024 – 14 stycznia 2025. Dostarczają one następujące informacje:

- 1) Liczba odwiedzin (Total visits):
 - Łączna liczba odwiedzin: 203 w ciągu ostatnich 28 dni (do 14 stycznia 2025).
- 2) Dystrybucja urządzeń (Device distribution)
 - Procent wizyt z komputerów stacjonarnych: 82,76%.
 - Procent wizyt z urządzeń mobilnych: 17,24%.
- 3) Przegląd zaangażowania użytkowników (Engagement overview):
 - Ruch (Traffic): Łączna liczba interakcji użytkowników wynosi 7 (związane z innymi wskaźnikami).
 - Średnia liczba stron na wizyty (Pages / Visit): Użytkownicy oglądają średnio 2,41 strony podczas jednej wizyty.
 - Średni czas trwania wizyty (Visit Duration): Użytkownik spędza na stronie średnio 1 minutę i 14 sekund.
 - Wskaźnik odrzuceń (Bounce Rate): 42,77% użytkowników opuszcza stronę bez interakcji (np. bez przejścia na kolejną stronę).
- 4) Ranking witryny (Rankings):
 - Global rank, Country rank oraz Industry rank: Brak danych o pozycji w rankingu globalnym.

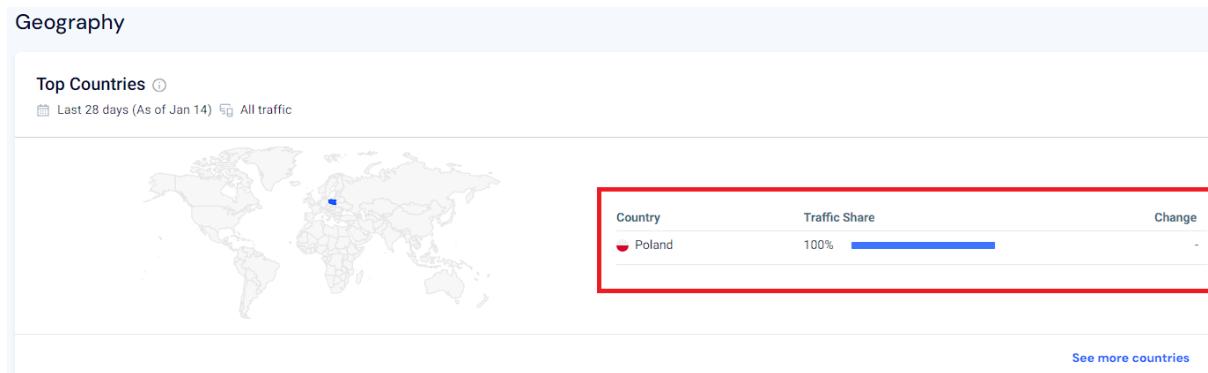


Obraz 13. Ciąg dalszy wyników wyszukiwania domeny na pro.similarweb.com

Dodatkowa analiza zakładki “Visits over time” w SimilarWeb (Obraz 13.) pozwala prześledzić codzienny rozkład ruchu na stronie integracje-ambiente.pl z okresu 18 grudnia 2024 – 14 stycznia 2025. Z wykresu wynika, że:

- Początkowo liczba wizyt była bardzo niska.
- Wzrost nastąpił około 20 grudnia, utrzymując się na poziomie 7 wizyt dziennie.
- W okolicy przełomu roku (1 stycznia)auważalny jest wzrost liczby wizyt, po czym następuje spadek w kolejnych dniach.
- Pod koniec okresu analiza wskazuje stabilizację na niskim poziomie.

W porównaniu z kilkoma innymi domenami o zbliżonym profilu (axel4x4.pl, drivingexperience.pl, autodrom4x4.pl) widoczne jest, że integracje-ambiente.pl plasuje się w średnim przedziale liczby wizyt – mniejszym niż drivingexperience.pl (840 wizyt), ale wyższym niż axel4x4.pl (22 wizyty).

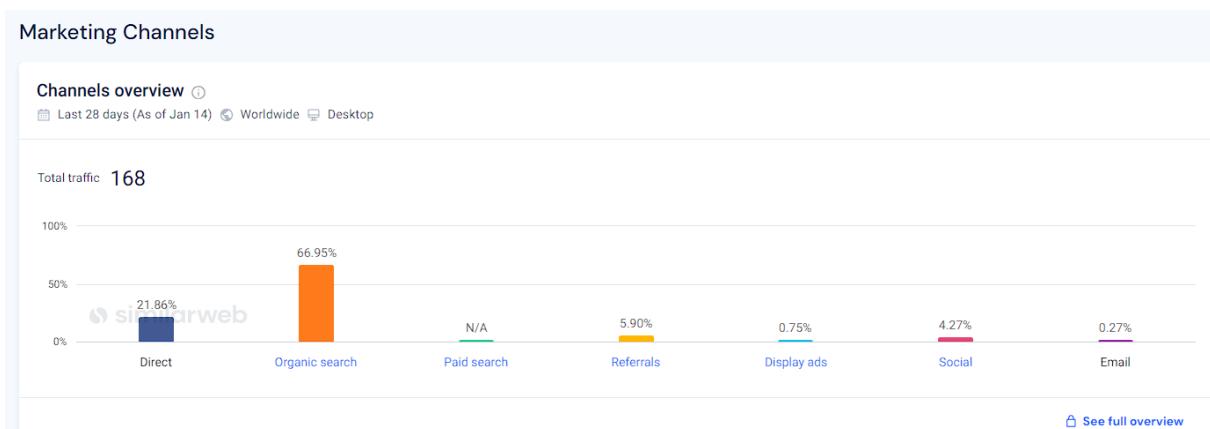


Obraz 14. Ciąg dalszy wyników wyszukiwania domeny na pro.similarweb.com

Kolejny aspekt zaprezentowany przez SimilarWeb (Obraz 14.) dostarcza dane geograficzne dotyczące ruchu na analizowanej witrynie z okresu 14 grudnia 2024 – 14 stycznia 2025.

Dostarczają one następujące informacje:

1. Witryna jest w całości odwiedzana przez użytkowników znajdujących się w Polsce, co może wskazywać na lokalny charakter działalności witryny lub jej ograniczenie do polskiej grupy odbiorców.
2. Nie odnotowano ruchu z innych krajów, co może wynikać z braku działań międzynarodowych lub treści skierowanych wyłącznie do polskojęzycznych użytkowników.



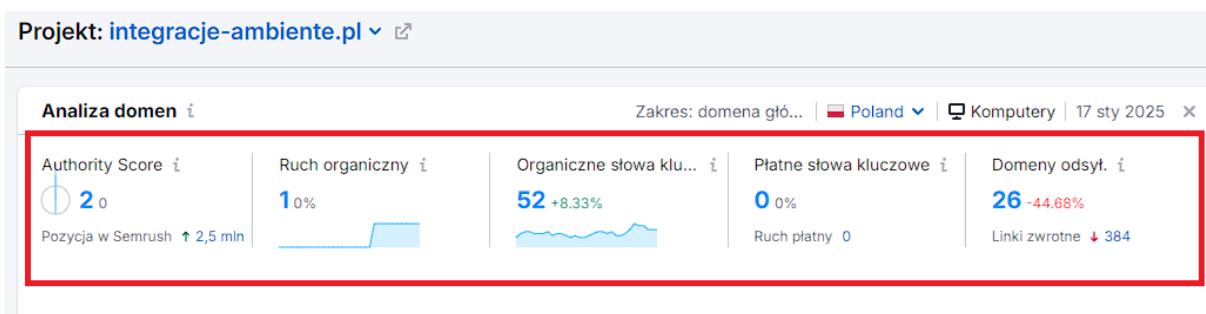
Obraz 15. Ciąg dalszy wyników wyszukiwania domeny na pro.similarweb.com

Kolejny fragment analizy SimilarWeb (Obraz 15.) prezentuje kanały, z których użytkownicy trafiają na witrynę integracje-ambiente.pl w okresie 14 grudnia 2024 – 14 stycznia 2025. Według tych danych:

1) Całkowity ruch: 168 odwiedzin.

2) Podział ruchu według kanałów:

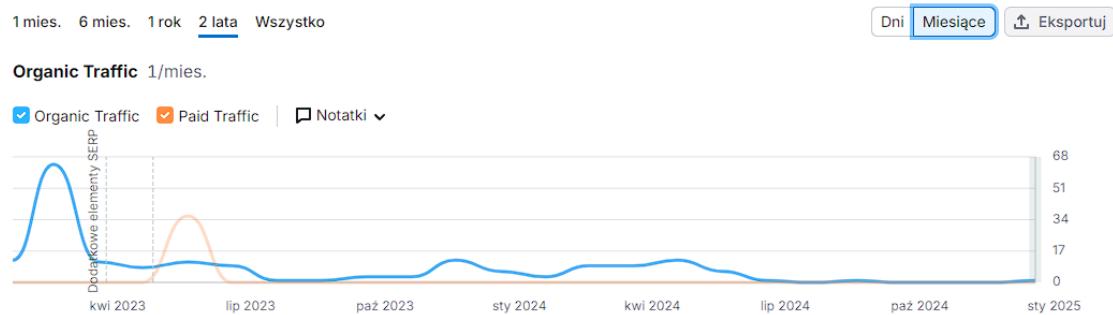
- Organic search (66,95%) – największy odsetek ruchu pochodzi z wyników wyszukiwania co sugeruje, że potencjalni klienci najczęściej odnajdują stronę, wpisując w wyszukiwarce słowa kluczowe związane z witryną
- Direct (21,86%) – ruch bezpośredni (np. wprowadzanie adresu w przeglądarce, zakładki, linki w wiadomościach) stanowi około jedną piątą. Oznacza to, że część odbiorców jest już świadoma marki lub posiada zapisany link.
- Referrals (5,90%) – niewielki, lecz zauważalny odsetek odwiedzin pochodzi z odnośników na innych witrynach
- Social (4,27%) – źródła mediów społecznościowych generują niewielki, ale potencjalnie istotny strumień ruchu.
- Display ads (0,75%) – niemal pomijalna wartość, co sugeruje niewielkie lub okazjonalne kampanie reklam banerowych w sieci.
- E-mail (0,27%) – śladowa ilość wizyt dociera przez linki w wiadomościach e-mail
- Paid search (N/A) – brak zarejestrowanego ruchu z płatnych kampanii w wyszukiwarkach



Obraz 16. Wyniki wyszukiwania domeny na semrush.com

Dodatkowe statystyki (Obraz 16.) pochodzą z analizy domeny w narzędziu SEMrush, które monitoruje pozycjonowanie stron w wyszukiwarkach. Wskazują one na:

- Authority Score: 2 – bardzo niski autorytet domeny (mała liczba wartościowych linków).
- Ruch organiczny: 1% – domena praktycznie nie pojawia się wysoko w wynikach wyszukiwania.
- Organiczne słowa kluczowe: 52 (+8,33%) – niewielki, lecz rosnący zasięg na frazy w Google.
- Płatne słowa kluczowe: 0% – brak kampanii w systemach typu Google Ads.
- Domeny odsyłające: 26 (spadek o 44,68%) – liczba backlinków znacząco zmalała, co pogarsza pozycjonowanie i wiarygodność witryny.



Obraz 17. Ciąg dalszy wyników wyszukiwania domeny na semrush.com

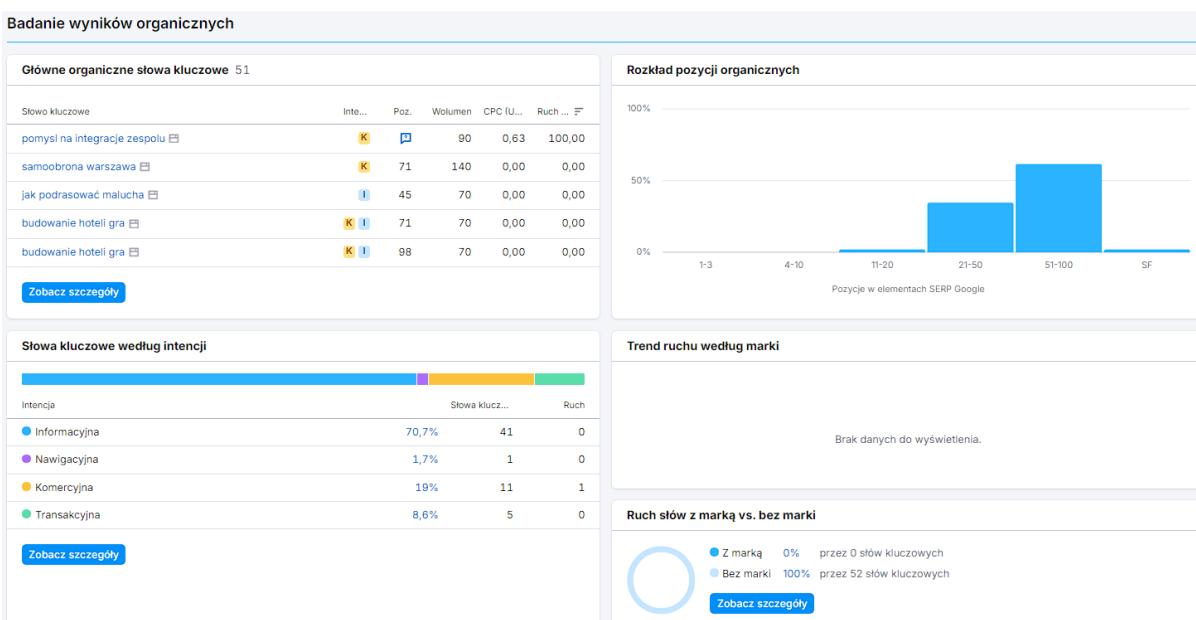
Rozszerzona analiza ruchu według SEMrush (Obraz 17.) z(okresu ostatnich 2 lat dostarcza następujące informacje na temat witryny domeny:

1) Ruch organiczny (linia niebieska):

- Widać gwałtowny wzrost ruchu organicznego w kwietniu 2023 roku, po którym następuje szybki spadek i stabilizacja na niskim poziomie.
- Od lipca 2023 roku ruch organiczny utrzymuje się na minimalnym poziomie (średnio 1 sesja miesięcznie), co wskazuje na bardzo niską popularność strony w wynikach wyszukiwania.

2) Ruch płatny (linia pomarańczowa):

- W okolicach kwietnia/maja 2023 r. pojawia się pojedynczy wzrost aktywności, co może odzwierciedlać krótką kampanię reklamową
- Po tym okresie linia jest praktycznie płaska, co sugeruje brak kontynuacji płatnych działań promocyjnych.



Obraz 18. Ciąg dalszy wyników wyszukiwania domeny na semrush.com

Uzupełniająca analiza wyników organicznych (Obraz 18.) dostarcza następujące dane:

1) Pozycje w SERP:

- Większość fraz plasuje się w zakresie 51–100 miejsca w wynikach wyszukiwania, co ogranicza szanse na kliknięcia.
- Pojedyncze słowa kluczowe są notowane w przedziale 21–50, natomiast brak pozycji w TOP 10.

2) Rodzaj fraz (intencja):

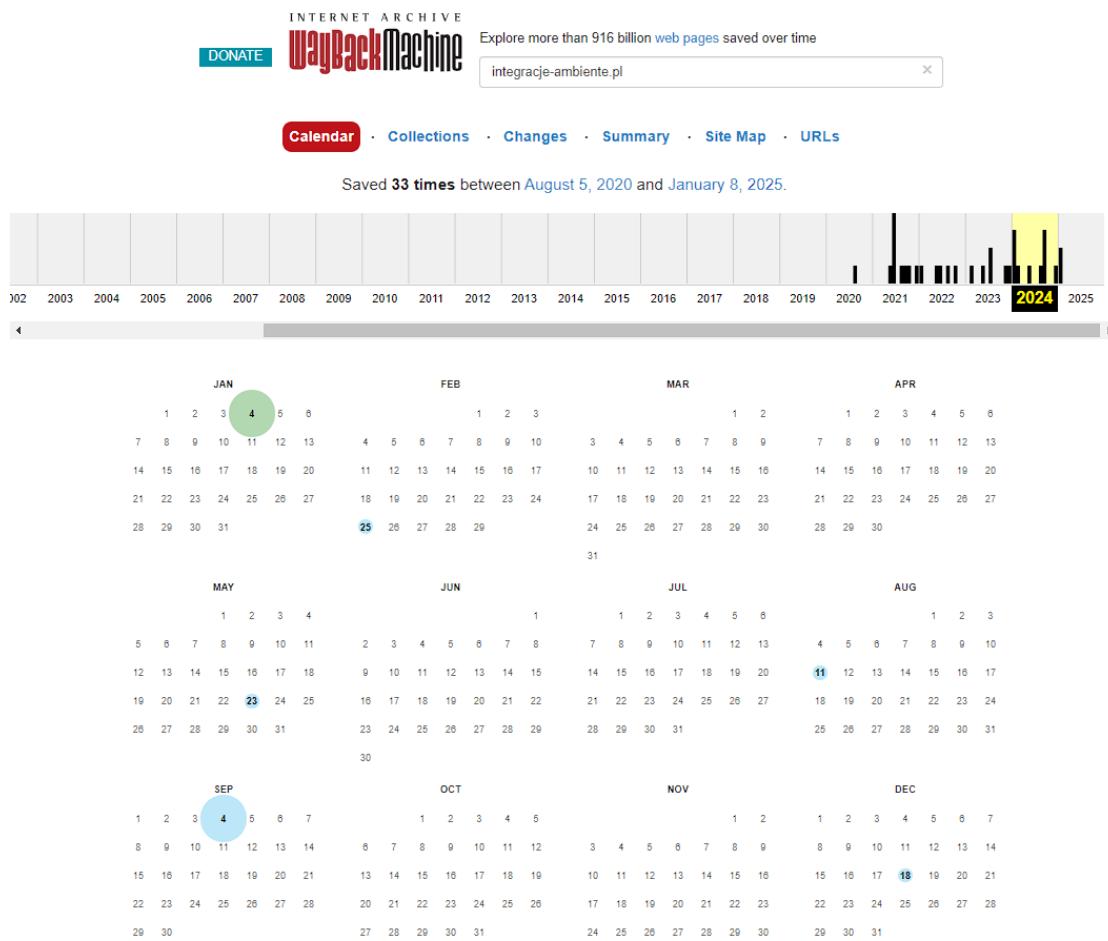
- 70,7% to zapytania informacyjne (np. „pomysł na integrację zespołu”),
- 19% komercyjne,

- c) 8,6% transakcyjne,
- d) 1,7% nawigacyjne.
- e) Brak fraz ścisłe związanych z rozpoznawalnością marki („z marką” = 0%).

3) Przykładowe słowa kluczowe:

- a) „pomysł na integrację zespołu” (pozycja 90)
- b) „samoobrona warszawa” (pozycja 71)
- c) „budowanie hotelu gra” (pozycja 71)

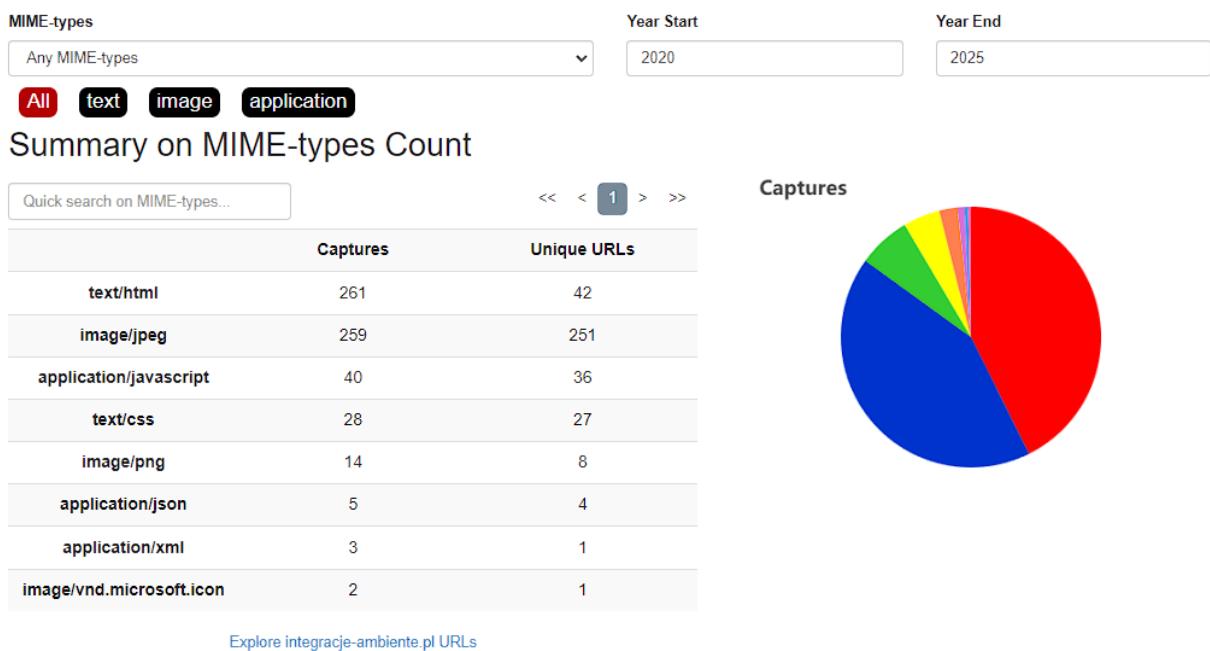
IV.2. Intensywność modyfikacji strony



Obraz 19. Wynik wyszukiwania domeny na web.archive.org

W celu określenia, jak często zmienia się zawartość witryny integracje-ambiente.pl, przeanalizowano jej historię w Wayback Machine (archive.org). Z zarejestrowanych w archiwum danych (Obraz 19.) wynika, że:

- 1) Liczba zapisów: Strona została zachowana 33 razy w okresie od 5 sierpnia 2020 r. do 8 stycznia 2025 r..
- 2) Rozkład w czasie:
 - Największe zagęszczenie snapshotów przypada na lata 2022–2024, co sugeruje, że w tym okresie dokonano zauważalnych zmian lub po robot Wayback Machine częściej odwiedzał stronę.
 - W niektórych miesiącach brak jakichkolwiek nowych zapisów, co może oznaczać dłuższe okresy bez istotnych modyfikacji.



Obraz 20. ciąg dalszy wyników wyszukiwania domeny na web.archive.org

Obraz (Obraz 20.) przedstawia statystyki dotyczące liczby zapisów różnych typów plików (MIME types) związanych ze stroną "integracje-ambiente.pl" w latach 2020–2025. Zawiera zarówno tabelaryczne zestawienie typów MIME, jak i wykres kołowy przedstawiający ich procentowy udział. Opis wyników:

Typy MIME i ich liczba zapisów:

- 1) text/html:
 - a) Liczba zapisów: 261.
 - b) Liczba unikalnych URL: 42.
 - c) HTML dominuje w zapisywanych zasobach, co oznacza częste zmiany w strukturze lub treści strony.
- 2) image/jpeg:
 - a) Liczba zapisów: 259.
 - b) Liczba unikalnych URL: 251.
 - c) Duża liczba obrazów JPEG wskazuje na bogatą zawartość graficzną strony.

- 3) application/javascript:
 - a) Liczba zapisów: 40.
 - b) Liczba unikalnych URL: 36.
 - c) Wskazuje na obecność dynamicznych elementów strony, np. interaktywnych funkcji.
- 4) text/css:
 - Liczba zapisów: 28.
 - Liczba unikalnych URL: 27.

Stylowanie strony było stosunkowo stabilne, z niewielkimi zmianami w arkuszach stylów.
- 5) image/png:
 - Liczba zapisów: 14.
 - Liczba unikalnych URL: 8.

Mniej popularny format graficzny w porównaniu do JPEG.
- 6) application/json oraz application/xml:
 - a) Liczba zapisów: 5 i 3 odpowiednio.
 - b) Wskazuje na ograniczone wykorzystanie API lub danych strukturalnych.
- 7) image/vnd.microsoft.icon:
 - a) Liczba zapisów: 2.
 - b) Liczba unikalnych URL: 1.

IV.3. Usługi świadczone dla klientów



Obraz 21. integracje-ambiente.pl strona główna

Imprezy w plenerze

- OFF-ROAD
- Survival
- Maluch Tuning Championship
- Gry strategiczne i integracje
- Paintball
- Gry miejskie
- Programy team-building
- Kreatywne
- Warsztaty
- Spływy kajakowe
- Bezludna Wyspa

Imprezy w hotelu

- Wieczory tematyczne
- Gry strategiczne i integracje
- Pokazy, występy Gwiazd
- Maszyna Goldberga
- Escape Room
- Warsztaty kulinarne, barmańskie, baristyczne
- Warsztaty eko, kreatywne
- Degustacje
- Samoobrona, zajęcia sportowe

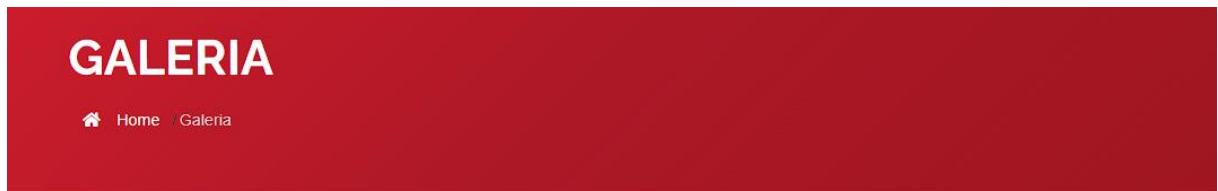
Obraz 22. integracje-ambiente.pl strona główna ciąg dalszy

Witryna udostępnia opis kategorii imprez (plener, hotel, off-road, pikniki) wraz z przykładowymi atrakcjami. Dzięki temu klient może wstępnie zapoznać się z zakresem usług bezpośrednio na stronie. (Obraz 22. Oraz 23.)



Obraz 23. integracje-ambiente.pl zakładka kontakt

Formularz kontaktowy umożliwia łatwe przesyłanie zapytań o wycenę lub szczegółowe informacje. Klient wypełnia pola (imię i nazwisko, adres e-mail, temat zapytania, treść wiadomości), a odpowiedź otrzymuje mailowo. (Obraz 24.).



Obraz 24. integracje-ambiente.pl zakładka galeria

Strona prezentuje zdjęcia z dotychczasowych imprez, co pomaga klientom w ocenie jakości i charakteru organizowanych eventów. (Obraz 25.).

IV.4. Podsumowanie

W rozdziale IV dokonano analizy danych dotyczących funkcjonowania witryny integracje-ambiente.pl, jej popularności, oferowanych funkcji oraz intensywności aktualizacji. Na podstawie zebranych informacji można stwierdzić, że strona spełnia swoją podstawową rolę jako narzędzie informacyjne i kontaktowe, jednak jej efektywność marketingowa oraz widoczność w sieci są ograniczone. Poniżej podsumowano najważniejsze aspekty:

- 1) Popularność i ruch na stronie
 - a) Witryna generuje niski ruch – w ostatnich 28 dniach zanotowano około 203 wizyt, co wskazuje na ograniczone zainteresowanie użytkowników.
 - b) Ruch pochodzi głównie z Polski (100%), co jest zgodne z lokalnym charakterem działalności firmy.
 - c) Najważniejszym źródłem ruchu jest wyszukiwanie organiczne (66,95%). Brak kampanii płatnych w wyszukiwarkach oraz niska liczba wejść z mediów społecznościowych sugerują ograniczoną aktywność firmy w zakresie płatnej reklamy i działań promocyjnych online.
- 2) Pozycjonowanie i słowa kluczowe
 - a) Strona jest widoczna w wynikach wyszukiwania dla 51 fraz kluczowych, z czego większość ma charakter informacyjny i nie prowadzi bezpośrednio do działań transakcyjnych.
 - b) Brak pozycji w TOP 10 oraz niewielka liczba backlinków (domen odsyłających) ograniczają widoczność witryny w wyszukiwarkach.
- 3) Intensywność modyfikacji
 - a) Dane z Wayback Machine i analizy MIME-types wskazują, że witryna była aktualizowana umiarkowanie często, głównie w latach 2022–2024.
 - b) Zmiany obejmowały dodawanie nowych zdjęć, uzupełnianie treści ofertowych i drobne modyfikacje skryptów (HTML, CSS, JavaScript).
- 4) Usługi świadczone przez witrynę
 - a) Strona oferuje prezentację ofert związanych z organizacją
 - b) Formularz kontaktowy pozwala na łatwe przesyłanie zapytań
 - c) Galeria zdjęć

Rozdział V Struktura domeny

V.1. Poddomeny

Subdomain	IP	Cloudflare
mail.integracje-ambiente.pl	195.246.126.117	
www.integracje-ambiente.pl	195.246.126.117	
autodiscover.integracje-ambiente.pl	none	
cpanel.integracje-ambiente.pl	none	
cpcalendars.integracje-ambiente.pl	none	
cpcontacts.integracje-ambiente.pl	none	
webdisk.integracje-ambiente.pl	none	
webmail.integracje-ambiente.pl	none	

Obraz 25. Wynik wyszukiwania domeny przez subdomainfinder.c99.nl

Subdomains	HOSTNAME	IP ADDRESS	Search subdomains...
www.integracje-ambiente.pl		195.246.126.117	
mail.integracje-ambiente.pl		195.246.126.117	
ftp.integracje-ambiente.pl		195.246.126.117	
autodiscover.integracje-ambiente.pl		N/A	
cpcalendars.integracje-ambiente.pl		N/A	
cpanel.integracje-ambiente.pl		N/A	
webdisk.integracje-ambiente.pl		N/A	
webmail.integracje-ambiente.pl		N/A	
cpcontacts.integracje-ambiente.pl		N/A	

Obraz 26. Wynik skanowania domeny na stronie pentest-tools.com

W wyniku skanowania domeny integracje-ambiente.pl (Obraz 26. I 27.) otrzymano następującą listę poddomen:

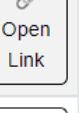
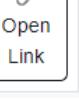
1) Lista poddomen:

- www.integracje-ambiente.pl - wskazuje na główną witrynę internetową.
- mail.integracje-ambiente.pl - przeznaczone do obsługi poczty e-mail.
- ftp.integracje-ambiente.pl - prawdopodobnie używane do przesyłania plików.
- autodiscover.integracje-ambiente.pl - konfiguracja automatyczna dla usług pocztowych
- cpcalendars.integracje-ambiente.pl - usługa synchronizacji kalendarzy

- cpanel.integracje-ambiente.pl - dostęp do panelu zarządzania serwerem.
- webdisk.integracje-ambiente.pl - służy do obsługi zdalnych zasobów dyskowych.
- webmail.integracje-ambiente.pl - interfejs WWW do obsługi poczty.
- cpcontacts.integracje-ambiente.pl - synchronizacja kontaktów.

2) Adresy IP:

- Poddomeny www, mail, i ftp wskazują na ten sam adres IP (195.246.126.117). Powtarzający się adres IP wskazuje, że usługi www, mail, i ftp działają na jednym serwerze.
- Pozostałe poddomeny nie mają przypisanego konkretnego adresu IP (oznaczone jako N/A).

#	SUBDOMAIN	IP/HOSTNAME	TYPE	STATUS	CLOUDFLARE	LINK
1	www.integracje-ambiente.pl	integracje-ambiente.pl	ALIAS	ONLINE	INACTIVE	 Open Link
2	mail.integracje-ambiente.pl	integracje-ambiente.pl	ALIAS	ONLINE	INACTIVE	 Open Link
3	cpanel.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link
4	webdisk.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link
5	webmail.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link
6	cpcontacts.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link
7	cpcalendars.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link
8	autodiscover.integracje-ambiente.pl	NOT FOUND	N/A	OFFLINE	N/A	 Open Link

Obraz 27. Wynik skanowania domeny przez subdomainfinder.in

W wyniku dalszego skanowania domeny integracje-ambiente.pl (Obraz 28.) otrzymano następujące wyniki:

- 1) Statusy poddomen:
 - ONLINE: Poddomeny www.integracje-ambiente.pl i mail.integracje-ambiente.pl są aktywne i dostępne.
 - OFFLINE: Poddomeny, takie jak cpanel, webdisk, webmail, cpcontacts, cpcalendars, oraz autodiscover, są niedostępne (OFFLINE).
- 2) Typy poddomen:
 - Poddomeny ONLINE mają status ALIAS, co oznacza, że są aliasami domeny głównej integracje-ambiente.pl. Oznacza to, że ich funkcjonalność może być kierowana na główną domenę.
 - Dla poddomen OFFLINE brak jest informacji o typie lub przypisanym IP.
- 3) Cloudflare:
 - Żadna z poddomen nie korzysta z usług Cloudflare (status INACTIVE), co może wpływać na brak dodatkowych zabezpieczeń, takich jak ochrona przed atakami DDoS czy optymalizacja wydajności.
- 4) Adres IP/Hostname:
 - Dla poddomen ONLINE wskazano adres integracje-ambiente.pl, co sugeruje wspólną konfigurację serwera dla głównych funkcji (WWW i mail).
 - Dla poddomen OFFLINE brak przypisanych hostów lub adresów IP (NOT FOUND).

V.2. Komputery w domenie i poddomenach

integracje-ambiente.pl subdomains			
Domain	Rank	Hosting Provider	Mail Provider
integracje-ambiente.pl		EXEA Sp. z o.o.	EXEA Sp. z o.o.
mail.integracje-ambiente.pl		EXEA Sp. z o.o.	-
ftp.integracje-ambiente.pl		EXEA Sp. z o.o.	-
www.integracje-ambiente.pl		EXEA Sp. z o.o.	-

Obraz 28. Wynik skanowania domeny przez securitytrails.com

A Records (subdomains from dataset)			
Host	IP	ASN	ASN Name
integracje-ambiente.pl	195.246.126.117 beta.3wdt.pl	ASN: 60713 195.246.126.0/23	TARRCI-AS, PL Poland

Obraz 29. Wynik skanowania domeny przez dnsdumpster.com

Analiza dostępnych informacji o komputerach w domenie integracje-ambiente.pl i jej poddomenach (Obraz 29. I Obraz 30. wskazuje na następujące szczegóły:

Domena integracje-ambiente.pl i jej dostępne poddomeny są obsługiwane przez firmę EXEA Sp. z o.o., która zapewnia zarówno hosting, jak i infrastrukturę sieciową. Sieć oparta jest na polskim dostawcy usług, co wskazuje na centralizację zasobów w lokalnych centrach danych.

Główne informacje o infrastrukturze:

- 1) Adres IP: 195.246.126.117 – przypisany do głównej domeny oraz aktywnych poddomen (www, mail, ftp).
- 2) Blok adresów: 195.246.126.0/23, zarządzany przez sieć TARRCI-AS (ASN: 60713), należącą do EXEA Sp. z o.o.
- 3) Poddomeny aktywne:
 - www.integracje-ambiente.pl – główna witryna,
 - mail.integracje-ambiente.pl – obsługa poczty,
 - ftp.integracje-ambiente.pl – zarządzanie plikami.

V.3. diagramy struktury domeny



Obraz 30. Diagram struktury domeny wygenerowany przez dnsdumpster.com

Diagram struktury domeny integracje-ambiente.pl (Obraz 30.) przedstawia zależności pomiędzy domeną główną, jej poddomenami oraz usługami sieciowymi. Z analizy wynika:

1. Główna domena i przypisane usługi:
 - integracje-ambiente.pl pełni funkcję domeny głównej.
 - Adres IP: 195.246.126.117, który obsługuje witrynę, pocztę i inne usługi.
 - Wszystkie usługi są obsługiwane przez sieć TARRCI-AS (ASN: 60713) w Polsce, zarządzaną przez firmę EXEA Sp. z o.o..
- 2) DNS i serwery nazw:
 - Domena korzysta z dwóch serwerów nazw:
 - ns1.3wdt.pl – adres IP: 195.246.126.114
 - ns2.3wdt.pl – adres IP: 195.246.126.116
 - Serwery DNS odpowiadają za zarządzanie rekordami domeny i są kluczowe dla jej działania.
- 3) Usługi pocztowe (MX):
 - Rekord MX wskazuje na obsługę poczty przez domenę główną (integracje-ambiente.pl), co oznacza, że poczta e-mail jest skonfigurowana wewnętrznie.
- 4) Zależności sieciowe:
 - Wszystkie adresy IP należą do tego samego bloku adresów sieciowych 195.246.126.0/23, co wskazuje na centralizację zasobów w jednym dostawcy infrastruktury.

V.4. Podsumowanie

W rozdziale V przeanalizowano strukturę domeny integracje-ambiente.pl, jej poddomeny, przypisane komputery oraz zależności sieciowe. Na podstawie zebranych danych można wyciągnąć następujące wnioski:

- 1) Struktura domeny i poddomen:
 - a) Główna domena integracje-ambiente.pl i aktywne poddomeny (www, mail, ftp) są obsługiwane przez firmę EXEA Sp. z o.o..
 - b) Istnieje kilka technicznych poddomen (np. cpanel, webmail, autodiscover), które pozostają nieaktywne i prawdopodobnie nie są używane.
- 2) Adresy IP i infrastruktura:
 - a) Wszystkie aktywne usługi działają na jednym adresie IP (195.246.126.117), należącym do polskiej sieci TARRCI-AS zarządzanej przez EXEA Sp. z o.o.
 - b) Centralizacja zasobów w obrębie jednego serwera ułatwia zarządzanie, ale może stanowić potencjalne ograniczenie pod względem skalowalności i odporności na awarie.
- 3) DNS i serwery nazw:
 - a) Domena korzysta z dwóch serwerów DNS (ns1.3wdt.pl i ns2.3wdt.pl) przypisanych do różnych adresów IP (195.246.126.114 i 195.246.126.116), co zapewnia redundancję i stabilność działania.
- 4) Zależności i usługi:
 - a) Obsługa poczty (MX) i strony WWW jest zintegrowana z główną domeną, co upraszcza konfigurację i użytkowanie.
 - b) Wszystkie komponenty sieciowe są częścią jednego bloku adresów IP (195.246.126.0/23), co wskazuje na lokalizację w polskich centrach danych.

Struktura domeny jest prosta i oparta na centralnej infrastrukturze zarządzanej przez jednego dostawcę (EXEA Sp. z o.o.), co ułatwia zarządzanie, ale może zwiększać ryzyko w przypadku awarii lub ataków. Aktywne poddomeny wspierają podstawowe funkcje witryny, takie jak hosting WWW i obsługa poczty, brak szerszych danych na odnośnie nieaktywnych poddomen technicznych które są prawdopodobnie pozostałością standardowej konfiguracji serwera. Diagram struktury domeny potwierdza jej prostą, lecz funkcjonalną organizację, z pełną zależnością od jednego dostawcy infrastruktury.

Rozdział VI Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi

VI.1. Systemy operacyjne:

The screenshot shows a user interface for OS Detection. At the top, there is a green button labeled 'OS Detection'. Below it, under the heading 'Evidence', there is a red-bordered box containing the text 'Operating System' and 'Linux 4.4'. At the bottom, under the heading 'Details', there is some very small, illegible text.

Obraz 31. Wynik skanowania domeny przez pentest-tools.com

Basic Information

Reverse DNS	beta.3wdt.pl
Forward DNS	www.dynamic.lea24.pl , 3koszulki.3wdt.com , www.crm foformat lea24 pl , fartprodukttest lea24 pl , mail bako karton pl , ...
Routing	195.246.126.0/23 via TARRCI-AS, PL (AS60713)
OS	linux

Obraz 32. Wynik skanowania domeny przez search.censys.io

Na podstawie narzędzi app.pentest-tools.com i search.censys.io (Obraz 31. I 32.) zidentyfikowano, że serwery obsługujące domenę integracje-ambiente.pl działają na systemie operacyjnym Linux, z wykrytymi wersjami jąder wskazującymi na stabilną i szeroko stosowaną konfigurację:

1) Wersja systemu operacyjnego:

- Narzędzie app.pentest-tools.com wskazuje na system Linux 4.4, co sugeruje wykorzystanie jednej z wersji stabilnych jądra, popularnych w środowiskach serwerowych.
- Censys potwierdza, że system operacyjny to Linux, jednak bez szczegółowej wersji.

VI.2. Usługi sieciowe

Basic Information

Reverse DNS	beta.3wdt.pl
Forward DNS	www.dynamic.lea24.pl, 3koszulki.3wdt.com, www.crm foormat.lea24.pl, fartprodukttest.lea24.pl, mail.bako-karton.pl, ...
Routing	195.246.126.0/23 via TARRCI-AS, PL (AS60713)
OS	linux
Services (18)	21/FTP, 22/SSH, 25/SMTP, 53/DNS, 80/HTTP, 110/POP3, 143/IMAP, 443/HTTP, 465/SMTP, 587/SMTP, 993/IMAP, 995/POP3, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP

Obraz 33. Wynik wyszukiwania domeny przez search.censys.io

Evidence		
Port	State	Service
21	open	ftp
22	open	ssh
25	open	smtp
53	open	domain
80	open	http
110	open	pop3
143	open	imap
443	open	https
465	open	smtp
587	open	smtp
993	open	imaps
995	open	pop3s

Obraz 34. Wynik skanowania domeny przez app.pentest-tools.com

Na podstawie przeprowadzonych analiz za pomocą narzędzi app.pentest-tools.com i search.censys.io (Obraz 32. Oraz Obraz 34.), zidentyfikowano otwarte porty oraz usługi dostępne na serwerze obsługującym domenę integracje-ambiente.pl. Poniżej przedstawiono wykryte usługi:

- 1) Port 21 (FTP)
 - a) FTP (File Transfer Protocol) to usługa sieciowa, która umożliwia przesyłanie plików między serwerem a klientem. Jest związana bezpośrednio z obsługą zdalnych operacji plikowych przez sieć.

- 2) Port 22 (SSH)
 - a) SSH (Secure Shell) to usługa sieciowa pozwalająca na zdalne zarządzanie serwerem. Jest to sposób na bezpieczne nawiązywanie połączeń z serwerem w celu jego administracji.
- 3) Porty 25, 465, 587 (SMTP)
 - a) SMTP (Simple Mail Transfer Protocol) to protokół sieciowy do przesyłania e-maili. Porty te wskazują różne wersje tej usługi (zwykła, z zabezpieczeniem STARTTLS, szyfrowana SMTPS).
- 4) Port 53 (DNS)
 - a) DNS (Domain Name System) to usługa sieciowa odpowiedzialna za tłumaczenie nazw domenowych (np. integracje-ambiente.pl) na adresy IP. Jest to kluczowa część działania internetu.
- 5) Porty 80, 443 (HTTP/HTTPS)
 - a) HTTP (Hypertext Transfer Protocol) i HTTPS (HTTP Secure) to usługi sieciowe umożliwiające przesyłanie danych między serwerem a klientem w kontekście stron WWW.
- 6) Porty 110, 995 (POP3/POP3S)
 - a) POP3 (Post Office Protocol) i jego szyfrowana wersja POP3S to usługi sieciowe do pobierania poczty e-mail z serwera.
- 7) Porty 143, 993 (IMAP/IMAPS)
 - a) IMAP (Internet Message Access Protocol) i IMAPS (szyfrowana wersja) to usługi sieciowe do zarządzania e-mailami bezpośrednio na serwerze.
- 8) Dodatkowe porty HTTP (2082, 2083, 2086, 2087, 2095, 2096)
 - a) Te porty są typowe dla usług zarządzania serwerem, takich jak cPanel. Są one przykładami usług sieciowych pozwalających na administrację serwerem przez przeglądarkę.

VI.3. Aplikacje realizujące usługi sieciowe:

Host	IP	ASN	ASN Name	Open Services (from DB)
integracje-ambiente.pl	195.246.126.117	ASN 60713	TARCCI-AS, PL	ssh: SSH-2.0-OpenSSH_7.4 https: Apache title: Allpipe cn: allpipe.pl tech: WordPress:5.6.13 MySQL PHP Apache HTTP Server Divi:3.0.83
MX Records				
0 integracje-ambiente.pl	195.246.126.117	ASN 60713	TARCCI-AS, PL	ssh: SSH-2.0-OpenSSH_7.4 https: Apache title: Allpipe cn: allpipe.pl tech: WordPress:5.6.13 MySQL PHP Apache HTTP Server Divi:3.0.83
NS Records				
ns.3wdt.pl	195.246.126.116	ASN 60713	TARCCI-AS, PL	ssh: SSH-2.0-OpenSSH_7.4 http: Apache tech: Apache HTTP Server https: Apache cn: beta.3wdt.pl tech: Apache HTTP Server
ns1.3wdt.pl	195.246.126.114	ASN 60713	TARCCI-AS, PL	ssh: SSH-2.0-OpenSSH_7.4 http: Apache tech: Apache HTTP Server https: Apache cn: beta.3wdt.pl tech: Apache HTTP Server

Obraz 35. Wynik wyszukiwania domeny przez dnsdumpster.com

Server software and technologies	
443 / TCP	
Evidence	
Software / Version	
WordPress	CMS, Blogs
MySQL	Databases
PHP PHP	Programming languages
Apache HTTP Server	Web servers
NextGEN Gallery 3.2.23	Photo galleries, WordPress plugins

Obraz 36. Wynik skanowania domeny przez app.pentest-tools.com

Na podstawie wyników z narzędzi app.pentest-tools.com i dnsdumpster.com (Obraz 35. oraz Obraz 36), udało się zidentyfikować aplikacje realizujące kluczowe usługi sieciowe na serwerze obsługującym domenę integracje-ambiente.pl:

- 1) Apache HTTP Server
 - Funkcja: Serwer WWW obsługujący protokoły HTTP i HTTPS.
 - Zastosowanie: Dostarcza treści stron internetowych, w tym pliki HTML, CSS oraz dynamicznie generowane treści.
- 2) WordPress
 - Funkcja: CMS (Content Management System) zarządzający treścią na stronie.
 - Zastosowanie: Wykorzystywany do tworzenia, edycji i publikowania treści witryny.
- 3) MySQL
 - Funkcja: System zarządzania relacyjnymi bazami danych.
 - Zastosowanie: Przechowywanie danych dynamicznych związanych z działaniem CMS, takich jak treści stron, dane użytkowników czy konfiguracje.
- 4) SSH (OpenSSH 7.4)
 - Funkcja: Protokół do bezpiecznego zdalnego zarządzania serwerem.

VI.4. Podsumowanie

W rozdziale VI wykonano analizę wykorzystywanych systemów operacyjnych, usług sieciowych oraz aplikacji realizujących te usługi w domenie integracje-ambiente.pl dostarczyło to istotnych informacji na temat infrastruktury technicznej serwera. Serwery działają na systemie operacyjnym Linux, który zapewnia stabilność, bezpieczeństwo i elastyczność, co jest typowe dla środowisk serwerowych.

W zakresie usług sieciowych serwer obsługuje szeroki wachlarz protokołów, takich jak FTP, SSH, SMTP, IMAP, POP3, HTTP i HTTPS, co pozwala na efektywną obsługę poczty elektronicznej, hostingu WWW oraz administracji. Szczególną uwagę należy zwrócić na zastosowanie szyfrowanych wersji protokołów (IMAPS, SMTPS, HTTPS), co świadczy o dbałości o bezpieczeństwo transmisji danych.

Aplikacje realizujące usługi sieciowe obejmują kluczowe rozwiązania takie jak Apache HTTP Server (serwer WWW), WordPress (CMS) oraz MySQL (baza danych). Ich integracja wspiera dynamiczne generowanie treści, zarządzanie danymi oraz kompleksową obsługę strony internetowej. Obecność SSH umożliwia bezpieczne zdalne zarządzanie serwerem.

Rozdział VII Wykorzystywane technologie informatyczne

VII.1. Wykorzystywane technologie informatyczne

Site Technology (fetched 6 days ago)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Perl 	Perl is a high-level, general-purpose, interpreted, dynamic programming language	www.sec.gov , www.2nn.jp , www.internetdownloadmanager.com
XML	No description	www.virustotal.com , www.qwant.com , www.dailymail.co.uk
SSL 	A cryptographic protocol providing communication security over the Internet	www.linkedin.com , login.live.com
PHP 	PHP is supported and/or running	www.bleepingcomputer.com , www.majorgeeks.com , www.pixiv.net

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript 	Widely-supported programming language commonly used to power client-side dynamic content on websites	chatgpt.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
jQuery 	A JavaScript library used to simplify the client-side scripting of HTML	www.amazon.ca , www.amazon.in , base-contacts.afrai.com

Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

Technology	Description	Popular sites using this technology
WordPress Self-Hosted 	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	www.ironfx.com , www.thehostingheroes.com , iclass.eccouncil.org

Obraz 37. Wynik wyszukiwania domeny przez netcraft.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8 	UCS Transformation Format 8 bit	www.instagram.com , www.google.com , www.udemy.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5 	Latest revision of the HTML standard, the main markup language on the web	webmail.vinccihostels.com , mail.google.com , x.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.tiktok.com , www.bing.com , www.netflix.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
CSS Media Query	No description	www.imdb.com , www.paypal.com , www.bilibili.com
External 	Styles defined within an external CSS file	www.twitch.tv , csi.amazon.com , app.powerbi.com

Obraz 38. Wynik wyszukiwania domeny przez netcraft.com cd.

Na podstawie wyników z narzędzi netcraft.com (Obraz 37. oraz Obraz 38.), udało się zidentyfikować technologie informatyczne wykorzystywane w domenie integracje-ambiente.pl. Poniżej zaprezentowano kluczowe technologie oraz ich funkcjonalność:

- 1) Technologie po stronie serwera
 - PHP – Język skryptowy używany do generowania dynamicznych stron internetowych.
 - Perl – Język programowania interpretowany, wykorzystywany do ogólnych zastosowań.
 - XML – Technologia do przechowywania i transportu danych.
- 2) Technologie po stronie klienta
 - JavaScript – Język programowania umożliwiający dynamiczne treści na stronach.
 - jQuery – Biblioteka ułatwiająca manipulację elementami HTML oraz obsługę zdarzeń.
- 3) Frameworki i CMS
 - WordPress (Self-Hosted) – System zarządzania treścią oparty na PHP i MySQL.
- 4) Kodowanie znaków
 - UTF-8 – Format kodowania znaków używany do przechowywania i przesyłania tekstu w różnych językach.
- 5) Inne technologie front-endowe
 - HTML5 – Najnowsza wersja języka HTML, wykorzystywana do strukturyzowania treści na stronach.
 - CSS Media Query – Narzędzie umożliwiające dostosowanie stylów do urządzeń o różnych rozmiarach ekranu.

Evidence	
Software / Version	Category
WordPress	CMS, Blogs
MySQL	Databases
PHP	Programming languages
Apache HTTP Server	Web servers
NextGEN Gallery 3.2.23	Photo galleries, WordPress plugins
Autoptimize	WordPress plugins, Performance
jQuery	JavaScript libraries
Underscore.js 1.8.3	JavaScript libraries
jQuery Migrate 1.4.1	JavaScript libraries

Obraz 39. Wynik skanowania domeny przez app.pentest-tools.com

Na podstawie wyników z narzędzia app.pentest-tools.com (Obraz 40.), lista technologii wykorzystywanych w domenie integracje-ambiente.pl zostaje uzupełniona o następujące elementy:

- 1) Technologie po stronie serwera

- Apache HTTP Server – Serwer HTTP, obsługujący zapytania i dostarczający treści stron internetowych.
- PHP – Język skryptowy do generowania dynamicznych stron internetowych.
- MySQL – Relacyjna baza danych wspierająca zarządzanie i przechowywanie danych aplikacji.

2) Frameworki i CMS

- WordPress – System zarządzania treścią (CMS) oparty na PHP i MySQL, wykorzystywany do tworzenia i zarządzania stronami internetowymi.
- NextGEN Gallery 3.2.23 – Wtyczka WordPress do zarządzania galeriami zdjęć.
- Autoptimize – Wtyczka WordPress poprawiająca wydajność strony, optymalizując zasoby takie jak CSS, JavaScript i HTML.

3) Technologie po stronie klienta

- jQuery – Biblioteka JavaScript ułatwiająca manipulację elementami HTML i obsługę zdarzeń.
- jQuery Migrate 1.4.1 – Narzędzie wspierające starsze wersje jQuery.
- Underscore.js 1.8.3 – Biblioteka JavaScript dostarczająca dodatkowe funkcjonalności dla manipulacji danych i obiektów.

VII.2. Podsumowanie

W Rozdziale VII przeprowadzono analizę technologii informatycznych wykorzystywanych w domenie integracje-ambiente.pl. Zidentyfikowane technologie obejmują rozwiązania serwerowe i klienckie, a także narzędzia wspierające front-end oraz systemy zarządzania treścią (CMS). Zgromadzone informacje pozwalają sformułować następujące kluczowe wnioski:

- 1) Technologie po stronie serwera
 - PHP i Perl – języki skryptowe obsługujące dynamiczne generowanie treści.
 - Apache HTTP Server – serwer WWW obsługujący ruch HTTP/HTTPS.
 - MySQL – system zarządzania relacyjnymi bazami danych, wspierający dynamiczne operacje strony.
- 2) Technologie po stronie klienta
 - JavaScript – język programowania umożliwiający interaktywność na stronie.
 - jQuery i Underscore.js – biblioteki wspierające manipulację HTML oraz optymalizujące działanie front-endu.
- 3) Frameworki i CMS
 - Wykorzystanie WordPressa (self-hosted) jako systemu zarządzania treścią (CMS) pozwala na efektywne zarządzanie treścią strony. Dodatkowo zastosowano wtyczki, takie jak NextGEN Gallery do obsługi multimedialnych oraz Autoptimize do optymalizacji wydajności.
- 4) Technologie front-endowe
 - HTML5 – zapewnia strukturę strony.
 - CSS Media Query – umożliwia dostosowanie wyglądu witryny do różnych urządzeń.
- 5) Kodowanie znaków
 - UTF-8 – standard kodowania znaków, gwarantujący kompatybilność z wieloma językami.

Wszystkie zidentyfikowane technologie są zgodne z nowoczesnymi standardami i wspierają funkcjonalność strony internetowej. Całość zastosowanych rozwiązań świadczy o dbałości o wydajność, bezpieczeństwo oraz interaktywność witryny. Wykorzystanie systemów zarządzania treścią i wtyczek umożliwia łatwe rozwijanie i zarządzanie stroną w przyszłości.

Rozdział VIII Pracownicy i osoby powiązane

VIII.1. Uzyskane informacje dotyczące pracowników organizacji

Kontakt

Ambiente Marzena Tomasik

Budy Michałowskie 72, 96-316 Międzyborów

Email:

 marzena@integracje-ambiente.pl

Mobile:

 +48 695 351 513

 marzena@imprezy-integracyjne-ambiente.pl

Obraz 40. integracje-ambiente.pl strona główna

Na podstawie dostępnych danych ze strony (Obraz 40.), można zidentyfikować Marzenę Tomasik jako kluczową osobę powiązaną z działalnością domeny. Jej dane kontaktowe, takie jak adresy e-mail (marzena@integracje-ambiente.pl oraz marzena@imprezy-integracyjne-ambiente.pl) oraz numer telefonu, sugerują, że pełni ona rolę osoby odpowiedzialnej za kontakt z klientami oraz zarządzanie operacyjne.

Informacje

Witryna

<https://integracje-ambiente.pl/>

Branża

Organizowanie imprez

Wielkość firmy

2–10 pracowników

Rodzaj

Samozatrudniony(-a)

Obraz 41. Wyszukanie integracje ambiente na stronie linkedin.com

Analiza profilu firmy "Integracje Ambiente" na platformie LinkedIn (Obraz 41.) wskazuje, że jest to organizacja zajmująca się organizowaniem imprez, takich jak wyjazdy firmowe, imprezy integracyjne, szkolenia oraz konferencje. Firma działa w branży organizacji wydarzeń, a jej struktura organizacyjna obejmuje od 2 do 10 pracowników, co klasyfikuje ją jako małą firmę. Forma prowadzenia działalności została określona jako samozatrudnienie.

Obraz 42. Profil właściciela integracje ambiente na platformie linkedin.com

	owner Ekstremalne4x4.pl sty 2010 – obecnie · 15 lat 1 miesiąc Masovian District, Grodzisk Mazowiecki County, Poland
	Extremalne4x4 17 lat 1 miesiąc
	● Owner sty 2010 – obecnie · 15 lat 1 miesiąc Poland
	● Owner at Extremalne4x4.pl sty 2008 – obecnie · 17 lat 1 miesiąc
	Owner at Ambiente Integracje Ambiente Integracje sty 2010 – obecnie · 15 lat 1 miesiąc Poland
	Owner AMBIENTE Marzena Tomaszik sty 1992 – obecnie · 33 lata 1 miesiąc Grodzisk Mazowiecki

Wykształcenie

	University of Warsaw BUSINESS, MANAGEMENT, MARKETING, AND RELATED SUPPORT SERVICES
--	--

Obraz 43. dane dotyczące właściciela cd. (linkedin.com)

Na podstawie analizy dostępnych danych z portalu LinkedIn (Obraz 42. Oraz 43.) udało się zidentyfikować kluczową osobę powiązaną z firmą Integracje Ambiente. Właścicielem firmy jest Marzena Tomaszik, co zostało potwierdzone w jej profilu zawodowym. Pani Tomaszik zarządza działalnością w zakresie organizacji imprez integracyjnych oraz innych wydarzeń, co znajduje odzwierciedlenie w charakterze usług oferowanych przez firmę.

Jej profil na LinkedIn wskazuje na bogate doświadczenie zawodowe, obejmujące również inne przedsięwzięcia, takie jak Ekstremalne4x4.pl. Pani Tomaszik pełni funkcję właściciela firmy Ambiente Integracje od stycznia 2010 roku, a jej kariera obejmuje ponad trzy dekady działalności biznesowej w różnych sektorach. Wykształcenie na Uniwersytecie Warszawskim w zakresie zarządzania, marketingu oraz usług biznesowych podkreśla jej kompetencje w zarządzaniu oraz prowadzeniu przedsiębiorstw.

Obecność Pani Tomaszik na platformie LinkedIn wskazuje na jej zaangażowanie w budowanie profesjonalnych relacji oraz otwartość na współpracę z klientami i partnerami biznesowymi.

The screenshot shows a LinkedIn profile for Jakub Brzeziński. At the top is a large profile picture placeholder. Below it, the name "Jakub Brzeziński" is displayed in bold. To the right, there are two university logos: the University of Łódź (red square) and the Jagiellonian University in Krakow (blue shield). Below the name, the title "Assistant Professor at Department of Logistics, Faculty of Management, University of Lodz" is shown. Underneath that, the location "Warszawa i okolice" and contact information ("Informacje kontaktowe", "194 obserwujących", "195 kontaktów") are listed. A blue button labeled "Dołącz, aby wyświetlić profil" (Join to view profile) is visible. At the bottom, a blue button labeled "Wiadomość" (Message) with a paper airplane icon is shown. The background of the profile page features a scenic forest landscape.

Obraz 44. Konto jednego z pracowników na platformie linkedin.com

Doświadczenie



Uniwersytet Łódzki

7 lat 4 mies.

- **Assistant Professor**

Pełny etat

lut 2024 –obecnie · 1 rok

- **assistant**

paź 2017 – lut 2024 · 6 lat5 mies.

Łódź, woj. łódzkie, Polska



Event Manager

Integracje Ambiente

lut 2016 –obecnie · 9 lat



Event Manager

Extremalne4x4

lut 2016 –obecnie · 9 lat

Wykształcenie



Uniwersytet Jagielloński w Krakowie

Postgraduate Degree, Contract law in consumer and professional trade

lut 2021 – lut 2022



Uniwersytet Łódzki

Master of Laws - LLM, Law

2011 – 2019

[Pokaż wszystkie informacje o wykształceniu \(4\) →](#)

Obraz 45. Informacje dotyczące jednego z pracowników cd. (linkedin.com)

Na podstawie analizy danych z portalu LinkedIn (Obraz 44. Oraz Obraz 45.) udało się zidentyfikować jednego z kluczowych pracowników firmy Integracje Ambiente. Jakub Brzeziński pełni funkcję Event Managera, co wskazuje na jego zaangażowanie w organizację wydarzeń integracyjnych i firmowych. Został on powiązany z firmą od lutego 2016 roku, a jednocześnie zajmuje podobne stanowisko w firmie Ekstremalne4x4.

Jego profil na LinkedIn podkreśla zarówno szerokie doświadczenie zawodowe, jak i solidne wykształcenie. Brzeziński ukończył studia prawnicze na Uniwersytecie Łódzkim, uzyskując tytuł magistra prawa w latach 2011–2019, a także studia podyplomowe na Uniwersytecie Jagiellońskim w zakresie prawa kontraktowego w handlu konsumenckim i zawodowym w latach 2021–2022. Od 2017 roku związany jest również z Uniwersytetem Łódzkim, gdzie początkowo pełnił funkcję asystenta, a od 2024 roku pracuje jako Assistant Professor w Katedrze Logistyki na Wydziale Zarządzania.

Obraz 46. Profil Marzeny Tomasik na platformie facebook.com

Obraz 47. Profil Jakuba Brzezińskiego na platformie facebook.com

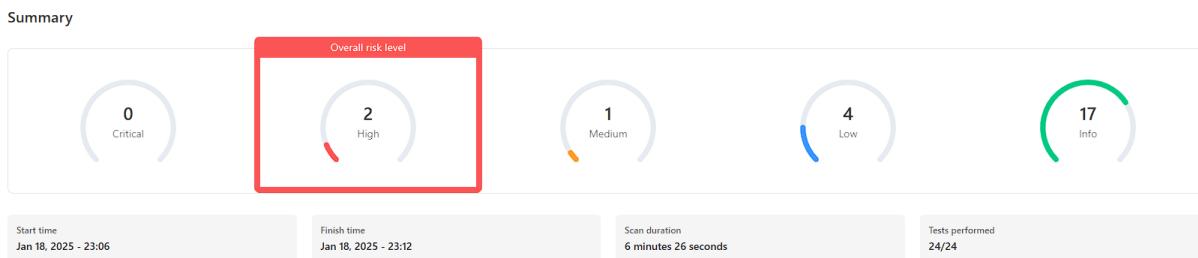
Na podstawie publicznie dostępnych profili na Facebooku (Obraz 46. Oraz Obraz 47.) zidentyfikowano dodatkowe informacje dotyczące zainteresowań i działalności osób powiązanych z firmą Integracje Ambiente. Profile Marzeny Tomasik i Kuby Brzezińskiego dostarczają szczegółowych danych o ich zainteresowaniach oraz aktywności poza zawodową.

VIII.2. Podsumowanie

Rozdział VIII dostarcza informacji na temat pracowników i osób powiązanych z firmą Integracje Ambiente. Na podstawie dostępnych danych z portali LinkedIn oraz Facebook zidentyfikowano kluczowe osoby związane z działalnością firmy, w tym właścicielkę Marzenę Tomasik oraz pracownika Kubę Brzezińskiego. Analiza ich profili pozwoliła na poznanie ich doświadczenia zawodowego, wykształcenia oraz zainteresowań prywatnych. Informacje te uzupełniają obraz działalności firmy i jej zespołu, podkreślając ich zaangażowanie zarówno w aspekcie zawodowym, jak i osobistym.

Rozdział IX Bezpieczeństwo

IX.1. Stwierdzone podatności



Obraz 48. Wynik skanowania domeny przez app.pentest-tools.com

Vulnerabilities found for Openssh 8.0				Unconfirmed
22 / TCP				
Risk Level	CVSS	CVE	Summary	Exploit
H	9.8	CVE-2023-38408	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.	N/A
M	6.8	CVE-2020-15778	scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."	N/A
M	6.5	CVE-2023-51385	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	N/A
M	5.9	CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP).	N/A

Obraz 49. Wynik skanowania domeny przez app.pentest-tools.com cd.

Vulnerabilities found for NextGEN Gallery 3.2.23				
443 / TCP				
Evidence				
Risk Level	CVSS	CVE	Summary	Exploit
H	8.8	CVE-2023-48328	Cross-Site Request Forgery (CSRF) vulnerability in Imagely WordPress Gallery Plugin – NextGEN Gallery allows Cross Site Request Forgery. This issue affects WordPress Gallery Plugin – NextGEN Gallery; from n/a through 3.37.	N/A
H	7.5	CVE-2023-3154	The WordPress Gallery Plugin WordPress plugin before 3.39 is vulnerable to PHAR Deserialization due to a lack of input parameter validation in the 'gallery_edit' function, allowing an attacker to access arbitrary resources on the server.	N/A
H	7.2	CVE-2023-3155	The WordPress Gallery Plugin WordPress plugin before 3.39 is vulnerable to Arbitrary File Read and Delete due to a lack of input parameter validation in the 'gallery_edit' function, allowing an attacker to access arbitrary resources on the server.	N/A
M	6.8	CVE-2020-35942	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload and Local File Inclusion via settings modification, leading to Remote Code Execution and XSS. (It is possible to bypass CSRF protection by simply not including a nonce parameter.)	N/A
M	5.3	CVE-2024-3097	The WordPress Gallery Plugin – NextGEN Gallery plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_item function in versions up to, and including, 3.59. This makes it possible for unauthenticated attackers to extract sensitive data including EXIF and other metadata of any image uploaded through the plugin.	N/A

Obraz 50. Wynik skanowania domeny przez app.pentest-tools.com cd.

M SSH service exposed to the Internet

22 / TCP

Evidence

We managed to detect a publicly accessible SSH service.

```

Starting Nmap ( https://nmap.org ) at 2025-01-19 00:11 EET
Nmap scan report for integracje-ambiente.pl (195.246.126.117)
Host is up (0.032s latency).

rDNS record for 195.246.126.117: beta.3wdt.pl

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     gssapi-keyex
|     gssapi-with-mic
|     password
|_    password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

```

Obraz 51. Wynik skanowania domeny przez app.pentest-tools.com cd.

L SPF record: Soft-fail ~all configuration

Confirmed

Evidence

Domain Queried	DNS Record Type	Description	Value
integracje-ambiente.pl	SPF	Sender Policy Framework	"v=spf1 ip4:195.246.126.117 +a +mx ~all"

Details

L DKIM record: default selectors found

Confirmed

Evidence

DKIM Selector	Key Type	Key Size	Value
default	rsa	1422	"v=DKIM1; k=rsa; p=MIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMiIBCgKCAQEAs5UYE3XJOjPK04CXITe5WfbnMrvbzh5amTPbVf7Xjb394jzSSEZfHksS03VqIUYaz3lRmShFvG2FrA39iOrr/F69Ey2HmlCQxsfd9ljbj9iC5nYbT0dthrshAJhceAt6V/Vow4RvCvMjfwr8H18O+38UeUhylOUzo9jSSyPcnVRFs4rZThbbApK+vFy8PxPK+JPOKJeQ9Liomj2HlrgBRs2mcP75KdmRgObchDu1dUzfO2k8cAormBjBljO+qBOWlDAQ

Obraz 52. Wynik skanowania domeny przez app.pentest-tools.com cd.

I FTP service exposed to the Internet

Confirmed

21 / TCP

Evidence

We managed to detect a publicly accessible File Transfer Protocol (FTP) service.

```

PORT      STATE SERVICE VERSION
21/tcp    open  ftp  Pure-FTPD

```

Details

I Missing DMARC policy

Confirmed

Evidence

We didn't find any TXT records associated with the target.

Details

Obraz 53. Wynik skanowania domeny przez app.pentest-tools.com cd.

Na podstawie przeprowadzonego skanowania domeny integracje-ambiente.pl (Obraz 48, Obraz 49, , Obraz 50 , Obraz 51 , Obraz 52, Obraz 53) zidentyfikowano kluczowe podatności, które mogą stanowić istotne zagrożenie dla bezpieczeństwa serwera i jego usług. Wyniki analizy podkreślają konieczność wdrożenia działań naprawczych w kilku krytycznych obszarach:

1) Podatności w OpenSSH 8.0:

- a) PKCS#11 (CVE-2023-38408): Luka umożliwia zdalne wykonanie kodu poprzez wykorzystanie niezaufanego klucza PKCS#11. Ryzyko: High (CVSS: 9.8)
- b) SCP Injection (CVE-2023-15778): Błąd walidacji argumentów w protokole SCP może prowadzić do nieautoryzowanej modyfikacji plików. Ryzyko: Medium (CVSS: 6.8).
- c) SSH Transport Vulnerability (CVE-2023-48795): Podatność na przechwytywanie pakietów przy specyficznych konfiguracjach rozszerzeń SSH. Ryzyko: Medium (CVSS: 5.9).

2) Podatności w NextGEN Gallery 3.2.23 (WordPress):

- a) Cross-Site Request Forgery (CSRF) (CVE-2023-48328): Luka umożliwia ataki CSRF, prowadząc do potencjalnej manipulacji danymi na serwerze. Ryzyko: High (CVSS: 8.8).
- b) PHAR Deserialization (CVE-2023-3154): Brak walidacji danych wejściowych w galerii zdjęć może prowadzić do nieautoryzowanego dostępu do zasobów serwera. Ryzyko: High (CVSS: 7.5).
- c) Luki w walidacji parametrów (CVE-2023-3155): Możliwość odczytu i modyfikacji danych w funkcji "gallery_edit". Ryzyko: High (CVSS: 7.2).

3) Dodatkowe zagrożenia:

- a) Publicznie dostępne usługi SSH i FTP: Obecność otwartych portów 22 (SSH) oraz 21 (FTP) bez dodatkowych mechanizmów ochrony zwiększa ryzyko nieautoryzowanego dostępu.
- b) Brak polityki DMARC: Niedostateczne zabezpieczenie systemu e-mail może prowadzić do wykorzystania domeny w atakach typu phishing lub spam.
- c) SPF z konfiguracją Soft-fail: Ograniczona skuteczność ochrony przed nieautoryzowanym wysyłaniem wiadomości.

Vulnerabilities

All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2023

CVE-2023-51767

70 OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

CVE-2023-51385

65 In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

CVE-2023-48795

59 The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.11 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 13.8b (and before 13.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.113, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

Obraz 54. Wynik skanowania domeny przez shodan.io

CVE-2023-38408

9.8 The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

📅 2021

CVE-2021-41617

7.0 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

CVE-2021-36368

3.7 An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."

📅 2020

CVE-2020-15778

7.8 scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

CVE-2020-14145

5.9 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

📅 2019

CVE-2019-16905

7.8 OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and local code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.

Obraz 55. Wynik skanowania domeny przez shodan.io cd.

📅 2016

CVE-2016-20012

5.3 OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

📅 2008

CVE-2008-3844

9.3 Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

📅 2007

CVE-2007-2768

4.3 OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

Obraz 56. Wynik skanowania domeny przez shodan.io cd.

Na podstawie wyników z shodan.io (Obraz 54, Obraz 55, , Obraz 56) przeprowadzono analizę potencjalnych podatności związanych z wykorzystaniem usługi OpenSSH w wersji 8.0 oraz innych usług wykrywanych w domenie integracje-ambiente.pl. Kluczowe wnioski to:

Stwierdzone podatności dla OpenSSH:

1) PKCS#11 (CVE-2023-38408):

- Wada w ścieżce zaufania ssh-agent przed wersją 9.3p2 może prowadzić do wykonania zdalnego kodu, gdy agent jest skierowany na system kontrolowany przez atakującego.
- Ocena ryzyka: 9.8 (krytyczna).

2) Command Injection (CVE-2023-15778):

- Wersje OpenSSH do 8.3p1 są podatne na wstrzyknięcie komend w funkcji scp.c, co umożliwia nieautoryzowane manipulowanie argumentami docelowymi.
- Ocena ryzyka: 7.8 (wysoka).

3) Integrity Bypass (CVE-2023-48795):

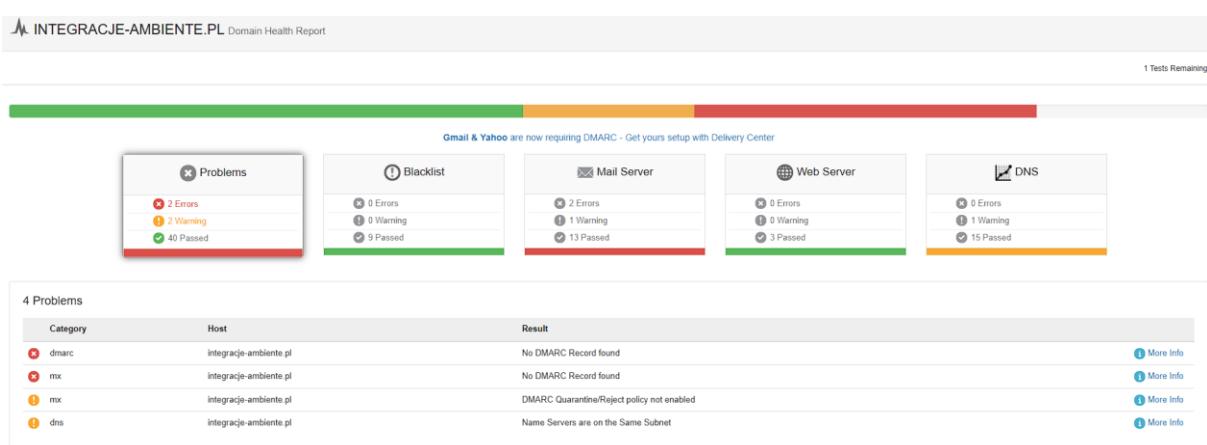
- Wersje OpenSSH przed 9.6 mogą pozwalać atakującym na ominięcie mechanizmów integralności poprzez błędne przetwarzanie fazy początkowej komunikacji w protokole SSH.
- Ocena ryzyka: 5.9 (średnia).

4) Command Injection w tokenach (CVE-2023-51385):

- Możliwość nieautoryzowanego uruchamiania komend poprzez metaznaki w nazwach użytkownika lub hosta.
- Ocena ryzyka: 6.5 (średnia).

5) Rowhammer (CVE-2023-51767):

- Atak wykorzystujący technikę "rowhammer" w pamięci DRAM może prowadzić do ominienia autoryzacji w wersjach OpenSSH do 9.6.
- Ocena ryzyka: 7.0 (wysoka).



Obraz 57. Wynik skanowania domeny przez mxtoolbox.com

Na podstawie analizy wykonanej za pomocą narzędzia mxtoolbox.com dla domeny integracje-ambiente.pl (Obraz 57.), zidentyfikowano następujące problemy związane z konfiguracją domeny:

1) Brak rekordu DMARC

- Domena nie posiada skonfigurowanego rekordu DMARC, który jest kluczowy dla ochrony przed phishingiem i spoofingiem e-mail. Brak DMARC naraża domenę na możliwość podszywania się pod nią (np. przez ataki phishingowe).

1) Brak rekordu DMARC w trybie Reject/Quarantine

- Rekord DMARC, o ile istnieje, nie jest skonfigurowany do stosowania restrykcyjnych polityk, takich jak odrzucanie nieautoryzowanych wiadomości. Fałszywe wiadomości mogą być dostarczane do skrzynek odbiorców, co zwiększa ryzyko oszustw e-mailowych.

2) Brak pełnej konfiguracji rekordów MX

- Rekordy MX, odpowiedzialne za kierowanie poczty e-mail, nie są w pełni skonfigurowane. Może to prowadzić do problemów z dostarczaniem e-maili i utrudniać funkcjonowanie usług pocztowych.

3) Serwery nazw znajdują się w tej samej podsieci

- Wszystkie serwery DNS znajdują się w tej samej podsieci, co oznacza, że awaria jednej podsieci może spowodować brak dostępu do DNS. Zmniejsza to redundancję i odporność na awarie.

IX.2. Złośliwe oprogramowanie

Safe Browsing site status

Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we discover thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers. You can search to see whether a website is currently dangerous to visit.

Check site status

integracje-ambiente.pl

Current status

No unsafe content found

Site info

This info was last updated on Jan 23, 2025.

Site safety can change over time. Check back for updates.

Obraz 58. Wynik wyszukiwania domeny na stronie transparencyreport.google.com

Na podstawie wyniku uzyskanego z narzędzia Google Safe Browsing Transparency Report (Obraz 58.), dotyczącego domeny [integracje-ambiente.pl](https://transparencyreport.google.com/safe-browsing/report?url=https://integracje-ambiente.pl), można wyciągnąć następujące wnioski:

- 1) Brak wykrycia złośliwego oprogramowania
- 2) Stan witryny:
 - Wynik analizy wskazuje, że na stronie nie wykryto żadnych niebezpiecznych treści, takich jak złośliwe oprogramowanie, phishing czy inne zagrożenia.
 - Witryna została oceniona jako bezpieczna do odwiedzenia.
- 3) Data ostatniej analizy:
 - Ostatnia aktualizacja wyników miała miejsce 23 stycznia 2025 roku.

 integracje-ambiente.pl

 No Malware Found
Our scanner didn't detect any malware

 Site is not Blacklisted
9 Blacklists checked

 Redirects to:
<https://integracje-ambiente.pl/>

IP address: 195.246.126.117
Hosting: Unknown
Running on: Apache

CMS: WordPress 5.3.18
Powered by: Unknown
[More Details](#)

Minimal Low Medium Security Risk High Critical

Our automated scan did not detect malware on your site. If you still believe that your site has been hacked, [sign up](#) for a complete scan, manual audit, and guaranteed malware removal.

Protection Recommendations
Directory Listing is [enabled](#) on your site. This can lead to information leakage. We recommend disabling Directory Listing, [learn how](#).

Website Malware & Security

- No malware detected by scan (Low Risk)
- No injected spam detected (Low Risk)
- No defacements detected (Low Risk)
- No internal server errors detected (Low Risk)
- Site is up to date (Low Risk); using WordPress 5.3.18

Website Blacklist Status

- Domain clean by Google Safe Browsing
- Domain clean by McAfee
- Domain clean by Sucuri Labs
- Domain clean by ESET
- Domain clean by PhishTank
- Domain clean by Yandex
- Domain clean by Onaxis

Obraz 59. Wynik wyszukiwania domeny na stronie sitecheck.sucuri.net

Your site does not appear to be blacklisted. If you still see security warnings on your site, [sign up](#) for a more complete scan, manual audit, and guaranteed blacklist removal.

 Website Monitoring
Not detected
[Learn More](#)

 Website Firewall
Not Detected
[Explore Sucuri Firewall](#)

Hardening Improvements

Protection
No website application firewall detected. Please install a cloud-based WAF to prevent website hacks and DDoS attacks.

Security Headers
Missing security header for ClickJacking Protection. Alternatively, you can use Content-Security-Policy: frame-ancestors 'none'.
Missing security header to prevent Content Type sniffing.
Missing Strict-Transport-Security security header.
Missing Content-Security-Policy directive. We recommend to add the following CSP directives (you can use default-src if all values are the same): script-src, object-src, base-uri, frame-src

Obraz 60. Wynik wyszukiwania domeny na stronie sitecheck.sucuri.net

Na podstawie analizy sitecheck.sucuri.net (Obraz 59. i Obraz 60.), domena integracje-ambiente.pl jest wolna od złośliwego oprogramowania i nie figuruje na czarnych listach. Jednak oceniono ją jako umiarkowanie ryzykowną z następujących powodów:

Kluczowe problemy:

- 1) Brak firewalla aplikacyjnego (WAF), co zwiększa podatność na ataki, takie jak DDoS.
- 2) Braki w nagłówkach bezpieczeństwa, w tym:
 - a) Ochrona przed clickjackingiem.
 - b) Strict Transport Security (HSTS) – brak wymuszania HTTPS.
 - c) Content Security Policy (CSP).

The screenshot shows the SiteCheck analysis for the domain `integracje-ambiente.pl`. The top bar indicates a 'Community Score' of 0 / 94. A note states 'No security vendors flagged this domain as malicious'. The analysis was performed 'a moment ago'. Below the main header, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION tab is selected, showing a message to 'Join our Community' and a table of security vendor analysis results. The table has two columns: vendor name and status ('Clean'). The vendors listed are: Abusix, ADMINUSLabs, AlienVault, Antiy-AVL, BitDefender, Certego, CINS Army, CRDF, Cyble, and desenmascara.me. All entries show a green checkmark and the word 'Clean'. There is also a column for 'Do you want to automate checks?' which contains a question mark icon.

Security vendor's analysis	Do you want to automate checks?
Abusix	<input checked="" type="checkbox"/> Clean
ADMINUSLabs	<input checked="" type="checkbox"/> Clean
AlienVault	<input checked="" type="checkbox"/> Clean
Antiy-AVL	<input checked="" type="checkbox"/> Clean
BitDefender	<input checked="" type="checkbox"/> Clean
Certego	<input checked="" type="checkbox"/> Clean
CINS Army	<input checked="" type="checkbox"/> Clean
CRDF	<input checked="" type="checkbox"/> Clean
Cyble	<input checked="" type="checkbox"/> Clean
desenmascara.me	<input checked="" type="checkbox"/> Clean

Obraz 61. Wynik wyszukiwania domeny na stronie virustotal.com

Na podstawie analizy virustotal.com (Obraz 61.), domena `integracje-ambiente.pl` została oceniona jako bezpieczna przez wszystkie 94 narzędzi bezpieczeństwa.

Kluczowe wnioski:

- 1) Brak wykrytego złośliwego oprogramowania lub innych zagrożeń.
- 2) Czysty status w systemach wielu dostawców zabezpieczeń, w tym BitDefender, AlienVault, CINS Army, i innych.

IX.3. Zagrożenia dla innych

Spam Database Lookup Results for 195.246.126.117

rDNS/PTR record for 195.246.126.117 is "beta.3wdt.pl".

Some mail servers will not accept mail from IP addresses with no rDNS/PTR record or a generic PTR record.

The following are blacklist test results. Being listed with a DNSBL does not always indicate the IP address is a source of spam. Some DNSBL's criteria are based of the IP address' country or connection type. If you are listed with a DNSBL click on the link for removal criteria.

all.s5h.net	b.barracudacentral.org	bl.0spam.org
pl.spamcop.net	blacklist.woody.ch	bogons.cymru.com
combined.abuse.ch	db.wpbl.info	dnsbl-1.uceprotect.net
dnsbl-2.uceprotect.net	dnsbl-3.uceprotect.net	dnsbl.dronebl.org
drone.abuse.ch	duinv.aupads.org	dyna.spamrats.com
ips.backscatterer.org	ix.dnsbl.manitu.net	korea.services.net
noptr.spamrats.com	orvedb.aupads.org	proxy.bl.gweep.ca
psbl.surriel.com	tbl.0spam.org	relays.bl.gweep.ca
relays.nether.net	singular.ttk.pte.hu	spam.abuse.ch
spam.dnsbl.anommails.de	spam.spamrats.com	spambot.bls.digibase.ca
spamrbl.imp.ch	spamsources.fabel.dk	ubl.lashback.com
ubl.unsubscribe.com	virus.rbl.jp	wormrbl.imp.ch
z.mailspike.net		

Obraz 62. Wynik wyszukiwania domeny na stronie dnsbl.info

Wyniki dnsbl.info (Obraz 62.) wskazują, że adres IP 195.246.126.117 nie znajduje się na żadnej z czarnych list DNSBL. Wszystkie testy blacklist w narzędziu dnsbl.info zakończyły się pozytywnie, co oznacza brak oznak użycia adresu IP w działaniach takich jak:

- 1) Wysyłanie spamu.
- 2) Działania złośliwe w sieci.
- 3) Wykorzystywanie jako serwer dla botnetów.
- 4) Brak wpisów na czarnych listach oznacza, że serwer nie był identyfikowany jako źródło podejrzanych działań, co wskazuje na jego wiarygodność w kontekście przesyłania poczty i ruchu sieciowego.

We resolved the domain integracje-ambiente.pl to IP address 195.246.126.117 ×

AbuseIPDB » 195.246.126.117

Check an IP Address, Domain Name, or Subnet
e.g. 2a02:a31d:e0ec:c200:a4ec:d41:5733:c811,
microsoft.com, or 5.188.10.0/24

195.246.126.117 was not found in our database

ISP	Domena.pl sp. z o.o.
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	beta.3wdt.pl
Domain Name	domena.pl
Country	Poland
City	Torun, Kujawsko-Pomorskie

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

[REPORT 195.246.126.117](#) [WHOIS 195.246.126.117](#)

IP Abuse Reports for 195.246.126.117:

This IP address has not been reported. [File Report](#)

Obraz 63. Wynik wyszukiwania domeny na stronie abuseipdb.com

Adres IP 195.246.126.117 nie został zgłoszony w bazie AbuseIPDB (Obraz 63.) jako źródło potencjalnych zagrożeń. Wyniki analizy wskazują na brak dowodów świadczących o zaangażowaniu serwera w działania mogące stanowić zagrożenie dla innych użytkowników

IX.4. Stosowane mechanizmy ochronne

SSL Report: integracje-ambiente.pl (195.246.126.117)

Assessed on: Sat, 25 Jan 2025 16:36:42 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating A

	Certificate	Protocol Support	Key Exchange	Cipher Strength
Certificate	100	100	100	100
Protocol Support	100	100	100	100
Key Exchange	100	100	100	100
Cipher Strength	100	100	100	100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Obraz 64. Wynik wyszukiwania domeny na stronie ssllabs.com

Raport SSL Labs dla domeny integracje-ambiente.pl (Obraz 64.) przyznał ocenę A, co świadczy o solidnym wdrożeniu standardów bezpieczeństwa.

Kluczowe elementy ochrony:

- 1) Certyfikat SSL: Poprawnie skonfigurowany, zapewniający szyfrowanie danych.
- 2) TLS 1.3: Obsługa najnowszej i najbezpiecznej wersji protokołu SSL/TLS.
- 3) Silne szyfrowanie i wymiana kluczy: Zgodne z nowoczesnymi standardami, co minimalizuje ryzyko ataków.
- 4) Zgodność z SNI: Wspiera hosting wielu certyfikatów na jednym adresie

Header	Description
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Obraz 65. Wynik wyszukiwania domeny na stronie securityheaders.com

Raport SecurityHeaders.com dla domeny integracje-ambiente.pl (Obraz 65.) przyznał ocenę F, co wskazuje na brak kluczowych nagłówków bezpieczeństwa w konfiguracji serwera. Brakujące nagłówki:

- 1) Strict-Transport-Security: Zalecany do wymuszania korzystania z HTTPS.
- 2) Content-Security-Policy: Chroni przed atakami XSS, ograniczając źródła ładowanych zasobów.
- 3) X-Frame-Options: Zabezpiecza przed atakami typu clickjacking.
- 4) X-Content-Type-Options: Zapobiega MIME-sniffingowi, wymuszając deklarowany typ zawartości.
- 5) Referrer-Policy: Kontroluje, jakie informacje o stronie są przesyłane w nagłówkach odsyłacza.
- 6) Permissions-Policy: Ogranicza dostęp do wybranych funkcji przeglądarki i interfejsów API.

IX.5. Podsumowanie

W rozdziale IX przeprowadzono kompleksową analizę bezpieczeństwa witryny integracje-ambiente.pl, skupiając się na stwierdzonych podatnościach, zagrożeniach, złośliwym oprogramowaniu oraz stosowanych mechanizmach ochronnych. Wyniki wskazują na obecność istotnych luk w zabezpieczeniach, które mogą wpłynąć na integralność oraz bezpieczeństwo danych i użytkowników.

Kluczowe wnioski:

- 1) Stwierdzone podatności:
 - a) Wykryto krytyczne i wysokie podatności w komponentach takich jak OpenSSH 8.0 oraz w wtyczce NextGEN Gallery dla WordPressa, które mogą umożliwić ataki typu RCE (Remote Code Execution) czy CSRF (Cross-Site Request Forgery). Zalecane jest natychmiastowe uaktualnienie tych elementów.
- 2) Złośliwe oprogramowanie:
 - a) Analizy za pomocą narzędzi (m.in. Google Safe Browsing, VirusTotal) nie wykazały obecności złośliwego oprogramowania ani działalności wskazującej na kompromitację witryny. Witryna nie została także zidentyfikowana jako źródło spamu.
- 3) Zagrożenia dla innych:
 - a) Sprawdzenia w bazach DNSBL oraz AbuseIPDB nie wykazały wpisów dotyczących aktywności związanej z rozsyłaniem spamu czy nieautoryzowaną działalnością na adresie IP przypisanym do domeny.
- 4) Stosowane mechanizmy ochronne:
 - a) Witryna uzyskała ocenę A w teście SSL Labs, co wskazuje na dobrą implementację protokołów TLS oraz konfigurację certyfikatów.
 - b) Jednak brak kluczowych nagłówków bezpieczeństwa (np. Strict-Transport-Security, Content-Security-Policy) stanowi istotne zagrożenie i wymaga natychmiastowych działań w celu poprawy ochrony.

Rozdział X Stosowane urządzenia sieciowe

X.1. Infrastruktura sieciowa

```
// 53 / TCP -186087355 | 2025-01-22T08:51:44.860215
PowerDNS Authoritative Server 4.9.2 (built Dec 20 2024 10:43:36 by root@bh-centos-8.dev.cpanel.net)
Resolver ID: beta.3wdt.pl

// 53 / UDP -186087355 | 2025-01-25T11:58:51.317219
PowerDNS Authoritative Server 4.9.2 (built Dec 20 2024 10:43:36 by root@bh-centos-8.dev.cpanel.net)
Resolver ID: beta.3wdt.pl
```

Obraz 66. Wynik skanowania domeny na stronie shodan.io

```
// 80 / TCP ↗
Apache httpd
Default Web Site Page
HTTP/1.1 200 OK
Date: Sat, 25 Jan 2025 11:20:18 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html
```

Obraz 67. Wynik skanowania domeny na stronie shodan.io cd.

```
// 465 / TCP
Exim smtpd 4.98
220-beta.3wdt.pl ESMTP Exim 4.98 #2 Thu, 02 Jan 2025 05:00:50 +0100
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
250-beta.3wdt.pl Hello 4s7ofk4bw26.org [224.97.167.172]
250-SIZE 52428800
250-LIMITS MAILMAX=1000 RCPTMAX=50000
250-8BITMIME
250-PIPELINING
250-PIPECONNECT
250-AUTH PLAIN LOGIN
250 HELP
```

Obraz 68. Wynik skanowania domeny na stronie shodan.io cd.

```
// 2087 / TCP
1367045288 | 2025-01-25T12:33:53.343Z

cp Logowanie do menedżera WHM
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Sat, 25 Jan 2025 12:33:53 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: whostmgrsession=%3a5UgNdtP6myvA7BLY%2cedb571fb2c47bc92aef7d54d4360d709; HttpOnly; path=/; port=2087; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=195.246.126.117; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; secur
e
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37882
```

Obraz 69. Wynik skanowania domeny na stronie shodan.io cd.

```
// 21 / TCP
Pure-FTPd

220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 200 allowed.
220-Local time is now 23:11. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
530 Login authentication failed
214-The following SITE commands are recognized
    ALIAS
    CHMOD
    IDLE
    UTIME
214 Pure-FTPd - http://pureftpd.org/
211-Extensions supported:
```

Obraz 70. Wynik skanowania domeny na stronie shodan.io cd.

```
// 995 / TCP
+OK Dovecot ready.
+OK
CAPA
TOP
UIDL
RESP-CODES
PIPELINING
AUTH-RESP-CODE
USER
SASL PLAIN LOGIN
*
```

Obraz 71. Wynik skanowania domeny na stronie shodan.io cd.

Na podstawie dostępnych danych z analizy pasywnej zidentyfikowano komponenty infrastruktury sieciowej domeny integracje-ambiente.pl. Informacje dotyczą głównie używanego oprogramowania i usług wirtualnych, natomiast brak jest szczegółowych danych dotyczących fizycznych urządzeń sieciowych, takich jak routery czy przełączniki. Poniżej przedstawiono wyniki analizy w kontekście urządzeń i infrastruktury sieciowej.

- 1) Router/DNS (Obraz 66.)
 - a) Serwery DNS opierają się na PowerDNS Authoritative Server 4.9.2, co wskazuje na zastosowanie rozwiązania open-source wdrożonego na serwerach wirtualnych lub dedykowanych. Brak szczegółowych danych na temat modeli routerów i urządzeń fizycznych obsługujących zapytania DNS.
- 2) Serwer WWW (Obraz 67.)
 - a) Ruch HTTP/HTTPS obsługiwany jest przez Apache HTTP Server, zainstalowany na serwerach zarządzanych przez operatora infrastruktury. Usługi te działają na systemie operacyjnym Linux, najprawdopodobniej na maszynach dedykowanych lub współdzielonych w centrach danych.
- 3) Serwery pocztowe (Obraz 68.)
 - a) Exim 4.98 obsługuje pocztę wychodzącą (SMTP). Zastosowanie tego rozwiązania wskazuje na środowisko serwerowe, jednak brak jest bezpośrednich informacji o fizycznych urządzeniach wspierających tę funkcjonalność.
- 4) Panel zarządzania serwerem (Obraz 69.)
 - a) cPanel/WHM jest używany do zarządzania konfiguracją serwerów, co sugeruje obecność standardowej infrastruktury hostingowej w centrach danych dostawcy.
- 5) Usługi FTP (Obraz 70.)
 - a) Pure-FTPD zapewnia obsługę protokołu FTP z szyfrowaniem TLS. Jest to rozwiązanie zoptymalizowane pod kątem wirtualnych środowisk serwerowych, bez ujawnionych szczegółów dotyczących urządzeń fizycznych.
- 6) Serwery IMAP/POP3 (Obraz 71.)
 - a) Dovecot obsługuje pocztę przychodzącą za pomocą protokołów IMAP/POP3, działając w ramach infrastruktury serwerowej.

X.2. Podsumowanie

Analiza wykonana w rozdziale VII wykazała, że infrastruktura sieciowa domeny integracje-ambiente.pl opiera się na wirtualnych usługach i oprogramowaniu open-source, takich jak PowerDNS, Apache, Exim, czy Dovecot, zarządzanych przez operatora hostingowego EXEA Sp. z o.o. w Polsce. Brak danych na temat fizycznych urządzeń sieciowych (routerów, przełączników) sugeruje, że są one skutecznie zabezpieczone przed dostępem publicznym. Informacje tego typu mogłyby być dostępne wyłącznie w wyniku aktywnych działań analitycznych, które wykraczają poza zakres rekonesansu pasywnego. Infrastruktura jest skoncentrowana w centrum danych dostawcy, co zapewnia centralne zarządzanie, ale może ograniczać widoczność na poziomie fizycznych urządzeń.

Rozdział XI Podsumowanie

Analiza domeny integracje-ambiente.pl przeprowadzona w ramach projektu umożliwiła uzyskanie kompleksowego obrazu jej infrastruktury, bezpieczeństwa oraz wykorzystanych technologii. Wyniki wskazują na poprawnie skonfigurowaną witrynę opartą na nowoczesnych rozwiązaniach, choć zidentyfikowano również obszary wymagające dalszej optymalizacji i wzmacnienia zabezpieczeń.

Domena integracje-ambiente.pl funkcjonuje w oparciu o infrastrukturę serwerową zarządzaną przez dostawcę usług hostingowych EXEA Sp. z o.o. w Polsce. Infrastruktura ta obejmuje serwer WWW oparty na Apache, system zarządzania treścią WordPress, a także komponenty wspierające, takie jak MySQL, Dovecot, Exim oraz PowerDNS. Wszystkie te elementy działają w środowisku Linux, co zapewnia elastyczność i niezawodność. Jednocześnie analiza wykazała brak szczegółowych danych dotyczących fizycznych urządzeń sieciowych, takich jak routery czy przełączniki, co może być efektem efektywnego ukrycia tych informacji przed dostępem publicznym.

W obszarze bezpieczeństwa domeny dostrzeżono zarówno jej mocne strony, jak i słabości. Wyniki wskazują na brak złośliwego oprogramowania oraz obecność ważnego certyfikatu SSL, który uzyskał wysoką ocenę w teście SSL Labs. Obsługa najnowszych protokołów szyfrowania, takich jak TLS 1.3, dodatkowo zwiększa bezpieczeństwo transmisji danych. Jednocześnie analiza wykazała istotne luki, w tym brak kluczowych nagłówków bezpieczeństwa, takich jak Strict-Transport-Security czy Content-Security-Policy, co obniża odporność na ataki typu XSS czy clickjacking. Wykryte podatności w komponentach OpenSSH i NextGEN Gallery podkreślają konieczność regularnych aktualizacji i monitorowania stanu infrastruktury.

W aspekcie konfiguracji poczty e-mail stwierdzono brak istotnych elementów, takich jak rekord DMARC, co może narazić domenę na wykorzystanie w atakach typu phishing. Dodatkowo analiza wskazuje na niedostatecznie skonfigurowane rekordy SPF, co zmniejsza skuteczność ochrony przed nieautoryzowanym wysyłaniem wiadomości e-mail. Pomimo tych braków, adres IP domeny nie został zidentyfikowany na czarnych listach ani w bazach zgłoszeń dotyczących nadużyć, co świadczy o jego dotychczasowej wiarygodności.

Pod względem wykorzystanych technologii, witryna opiera się na szerokim spektrum nowoczesnych rozwiązań, w tym PHP, HTML5, JavaScript oraz bibliotekach wspierających, takich jak jQuery. Zastosowanie wtyczek WordPressa, takich jak Autoptimize czy NextGEN Gallery, wzbogaca funkcjonalność witryny, choć jednocześnie wymaga szczególnej uwagi w zakresie aktualizacji i zabezpieczeń.