Spis treści:

1. Uzasadnienie wyboru domeny 3
2. Dane ogólne dotyczące organizacji 4
3. Serwery DNS obsługujące domenę 10
   https://who.is/ 10
   https://urlscan.io/domain/lidl.pl 12
   https://www.robtex.com/ 13
   https://dns.pl/whois 14
   https://www.whois.com/whois/lidl.pl 15
   https://www.virustotal.com/gui/ 16
   https://domainwat.ch/ 17
4. Ogólne informacje dotyczące witryny domeny 22
5. Struktura domeny 26
6. Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi 32
7. Wykorzystane technologie informatyczne 34
8. Pracownicy i osoby powiązane 36
9. Bezpieczeństwo 45
10. Stosowane urządzenia sieciowe 48
11. Źródła niesklasyfikowane 49
12. Inne 51
13. Wnioski ogólne 52

1. Uzasadnienie wyboru domeny.

Strona www.lidl.pl została przeze mnie wybrana, ponieważ często z niej korzystam. Jest to witryna oferująca zakupy internetowe w znanej sieci sklepów dyskontowych oraz przegląd aktualnej oferty sprzedażowej w sklepach stacjonarnych. Na stronie możemy uzyskać informacje o najnowszej ofercie spożywczej i tzw. sekcji Non-food (obejmującej artykuły gospodarstwa domowego, odzież, elektronikę, itp.). Możemy również sprawdzić godziny otwarcia każdego sklepu Lidl w Polsce. Jest to strona pozwalająca klientowi na zakupy internetowe oferty Noon-food, być na bieżąco z aktualnościami, a także posiadać użyteczne informacje o sklepie stacjonarnym (np. wspomniane godziny otwarcia) i wyrażenie własnej opinii odnośnie zakupów. Witryna wydawała mi się interesująca ze względu na różnorodność, począwszy od zakupów internetowych (proces logowania, rejestracji) poprzez przegląd oferty do podcastów i przepisów. Stwierdziłem, że taka ilość możliwości działań na stronie powinna pozwolić na dość ciekawy przebieg testu penetracyjnego.

Rys. 1. Wygląd badanej strony internetowej.

2. Dane ogólne dotyczące organizacji.

Zakres działania oraz historia organizacji:

Lidl, a dokładnie Lidl Stiftung & Co. KG jest to niemiecka sieć sklepów dyskontowych, działająca w 30 krajach. Główna siedziba przedsiębiorstwa znajduje się w Neckarsulm. Nazwa sieci pochodzi od nazwiska Ludwiga Lidla, emerytowanego nauczyciela. Lidl należy do Schwarz-Gruppe, która jest także właścicielem sieci sklepów „Kaufland".

Początki działalności sieci Lidl sięgają lat 30. XX wieku, kiedy to Josef Schwarz oraz Ludwig Lidl uruchomili firmę o nazwie Lidl & Schwarz Lebensmittel-Sortiments-Großhandel. W roku 1973 w Ludwigshafen am Rhein został otwarty pierwszy sklep o nazwie „Lidl". Piętnaście lat później, w roku 1988 Lidl w Niemczech miał już 460 filii i zatrudniał 5700 pracowników. W następnym roku powstał pierwszy sklep poza granicami Niemiec: we Francji. W roku 1990 otwarto sklep Lidla w Chemnitz, był to pierwszy sklep w nowych landach po zjednoczeniu Niemiec. W roku 1992 Lidl zintegrował się z siecią Nanz-Kette. W roku 1997 powstała strona internetowa Lidla. W roku 1999 Lidl jako pierwszy dyskont zainstalował skanery kasowe. W roku 2002 wszystkie sklepy zostały wyposażone w automaty do skupu butelek z kaucją (Pfandautomat). W roku 2003 w całej Europie pracowało w sieci Lidl 80 tysięcy pracowników. W roku 2008 do obrotu wprowadzono pieczywo wypiekane na miejscu: chleb bułki i croissanty. W roku 2009 Lidl po raz pierwszy otrzymał tytuł Händler des Jahres. Tytuł ten otrzymywał też kolejno w latach 2010–2013. W roku 2010 Lidl w Niemczech wprowadził dla swoich pracowników minimalną stawkę 10 €/godzinę. W roku 2012 do obrotu wprowadzone zostały produkty opatrzone marką Deluxe.

W sekcji polityka prywatności wyświetlane są następujące dane:

(Wersja 2.0; stan na 01.08.2019)

Polityka prywatności

Dziękujemy za zainteresowanie ochroną danych na naszej stronie internetowej. Chcemy, aby użytkownicy naszej strony czuli się na niej komfortowo i bezpiecznie, a ochronę danych postrzegali jako wyznacznik naszej jakości i dbałości o Klienta.
Poniższe wskazówki dotyczące ochrony danych zawierają informacje o rodzaju i zakresie przetwarzania Państwa danych osobowych przez spółkę **Lidl sp. z o.o. sp. k. ul. Poznańska 48 Jankowice, 62-080 Tarnowo Podgórne**. Dane osobowe to informacje, które są bezpośrednio lub pośrednio przyporządkowane albo możliwe do przyporządkowania do konkretnej osoby. Podstawę prawną ochrony danych stanowi w szczególności Rozporządzenie o ochronie danych osobowych (RODO).

Rys. 2. Początkowa polityka prywatności lidl.pl (zrzut ekranu).

Następnie wyświetlane są informacje odnośnie celu przetwarzania danych z przeglądarki użytkownika i o przebiegu oraz sposobie przechowywania uzyskanych danych.

1. Zestawienie
Wraz z wyświetleniem strony internetowej spółki Lidl sp. z o.o. sp. k. następuje wymiana różnych informacji między Państwa urządzeniem końcowym i naszym serwerem. Mogą to być również dane osobowe. Zgromadzone w ten sposób informacje są wykorzystywane m.in. do optymalizacji naszej strony internetowej lub do wyświetlania reklam w przeglądarce Państwa urządzenia końcowego.

2. Wyświetlanie naszej strony internetowej
Cel przetwarzania danych / podstawy prawne:
Podczas wyświetlania naszej strony internetowej działająca na Państwa urządzeniu końcowym przeglądarka bez Państwa udziału wysyła na serwer naszej strony i czasowo zapisuje w tzw. pliku dziennika:

- adres IP kompatybilnego z Internetem urządzenia, na którym jest wyświetlana strona,
- datę i godzinę wejścia,
- nazwę i adres URL wyświetlanego pliku,
- stronę / aplikację, z której nastąpiło wejście (adres URL strony),
- użytą przez Państwa przeglądarkę i ewentualnie system operacyjny Państwa komputera połączonego z Internetem oraz nazwę operatora Internetu

w następujących celach:

- zagwarantowanie niezakłóconego tworzenia połączenia,
- zagwarantowanie komfortowego korzystania z naszej strony internetowej / aplikacji,
- analiza bezpieczeństwa i stabilności systemu.

Rys. 3. Informacje o uzyskiwanych danych przez witrynę (zrzut ekranu).

W sekcji „Regulaminy” uzyskujemy informacje odnośnie numeru NIP, KRS, lokalizacje oraz dane teleadresowe.

I. Postanowienia ogólne

1. Niniejszy regulamin określa zasady dokonywania oraz realizacji zamówień towarów złożonych przez Klientów za pośrednictwem sklepu internetowego „lidl-sklep.pl”.
2. Właścicielem Sklepu jest spółka Lidl sp. z o.o. sp. k. z siedzibą w Jankowicach przy ul. Poznańskiej 48, gmina Tarnowo Podgórne (62-080), wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000597711, będąca zarejestrowanym podatnikiem od towarów i usług posiadająca numer identyfikacji podatkowej: NIP 7811897358 oraz numer statystyczny: REGON 302821772.
3. Klient korzystający ze Sklepu może kontaktować się z jego właścicielem za pośrednictwem poczty elektronicznej posiadającej adres info@lidl-sklep.pl lub pod numerem telefonu 800-012-071.
4. Sprzedawca za pośrednictwem Sklepu świadczy usługi:
a) zapoznania się z asortymentem Sklepu,
b) sprzedaży Produktów,
c) umożliwiania zamieszczania opinii o Sklepie przez Klientów,
d) prowadzenia Konta Klienta.

Rys. 4. Regulamin pkt. I (zrzut ekranu).

A także w zakładce „Kontakt” możemy uzyskać podobne, ale mniej obszerne dane.

Administrator danych:

Lidl sp. z o.o. sp. k.
ul. Poznańska 48, Jankowice
62-080 Tarnowo Podgórne

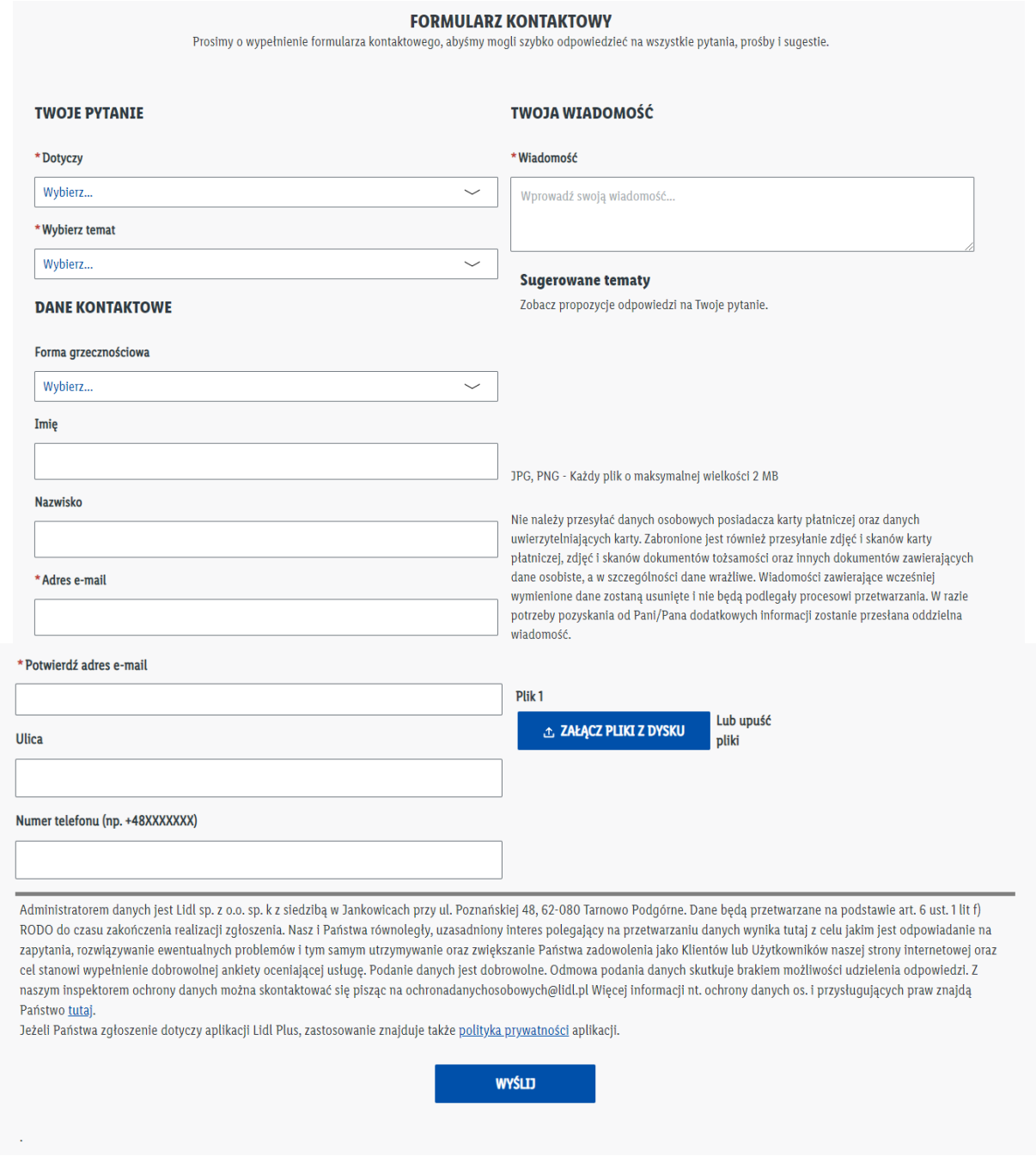
Spółka wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy Poznań-Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000597711, NIP: 781-18-97-358, REGON: 302821772

Rys. 5. Dane kontaktowe (zrzut ekranu).

BRANŻE

Działalność firm centralnych i doradztwo związane z zarządzaniem GŁÓWNA
Usługi prawnicze, rachunkowo-księgowe i doradztwo podatkowe
Usługi finansowe z wyłączeniem ubezpieczeń i funduszów emerytalnych
Obsługa rynku nieruchomości
Zatrudnienie
Administracja biurowa i wspomaganie prowadzenia działalności gospodarczej

Rys. 6. Branże kojarzone z siecią sklepów Lidl (zrzut ekranu – rejestr.io).



FORMULARZ KONTAKTOWY

Prosimy o wypełnienie formularza kontaktowego, abyśmy mogli szybko odpowiedzieć na wszystkie pytania, prośby i sugestie.

TWOJE PYTANIE

* Dotyczy

Wybierz...

* Wybierz temat

Wybierz...

DANE KONTAKTOWE

Forma grzecznościowa

Wybierz...

Imię

Nazwisko

* Adres e-mail

* Potwierdź adres e-mail

Ulica

Numer telefonu (np. +48XXXXXXX)

TWOJA WIADOMOŚĆ

* Wiadomość

Wprowadź swoją wiadomość...

Sugerowane tematy

Zobacz propozycje odpowiedzi na Twoje pytanie.

JPG, PNG - Każdy plik o maksymalnej wielkości 2 MB

Nie należy przesyłać danych osobowych posiadacza karty płatniczej oraz danych uwierzytelniających karty. Zabronione jest również przesyłanie zdjęć i skanów karty płatniczej, zdjęć i skanów dokumentów tożsamości oraz innych dokumentów zawierających dane osobiste, a w szczególności dane wrażliwe. Wiadomości zawierające wcześniej wymienione dane zostaną usunięte i nie będą podlegały procesowi przetwarzania. W razie potrzeby pozyskania od Pani/Pana dodatkowych informacji zostanie przesłana oddzielna wiadomość.

Plik 1

ZAŁĄCZ PLIKI Z DYSKU

Lub upuść pliki

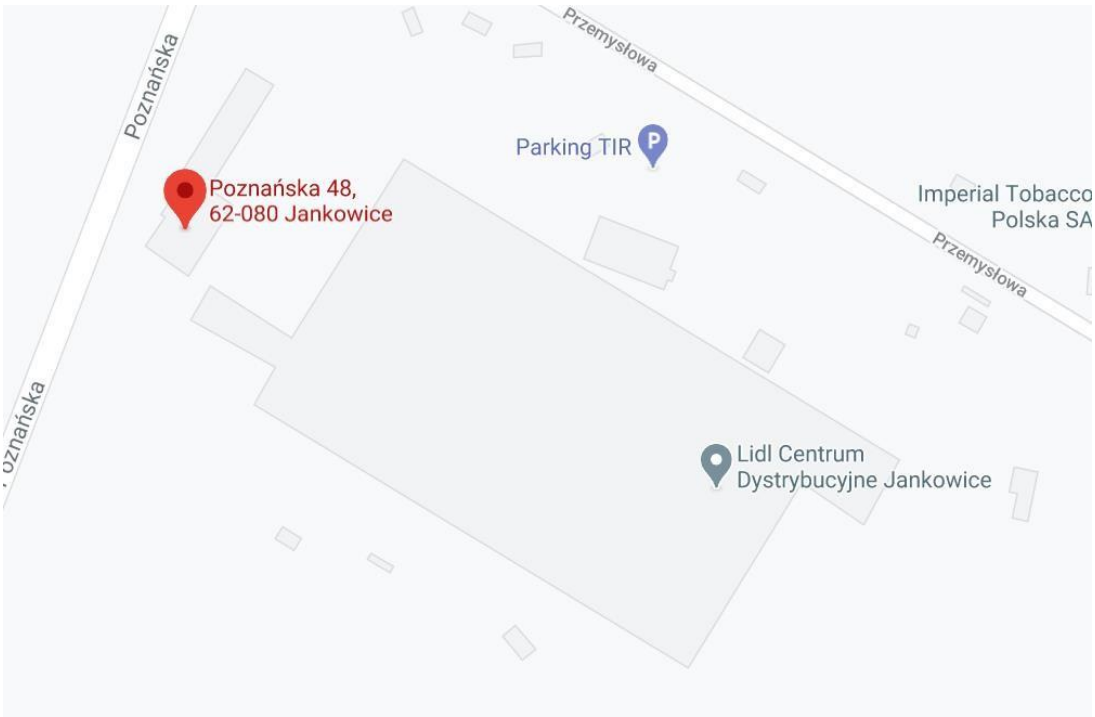
Administratorem danych jest Lidl sp. z o.o. sp. k z siedzibą w Jankowicach przy ul. Poznańskiej 48, 62-080 Tarnowo Podgórne. Dane będą przetwarzane na podstawie art. 6 ust. 1 lit f) RODO do czasu zakończenia realizacji zgłoszenia. Nasz i Państwa równoległy, uzasadniony interes polegający na przetwarzaniu danych wynika tutaj z celu jakim jest odpowiadanie na zapytania, rozwiązywanie ewentualnych problemów i tym samym utrzymywanie oraz zwiększanie Państwa zadowolenia jako Klientów lub Użytkowników naszej strony internetowej oraz cel stanowi wypełnienie dobrowolnej ankiety oceniającej usługę. Podanie danych jest dobrowolne. Odmowa podania danych skutkuje brakiem możliwości udzielenia odpowiedzi. Z naszym inspektorem ochrony danych można skontaktować się pisząc na ochronadanychosobowych@lidl.pl Więcej informacji nt. ochrony danych os. i przysługujących praw znajdą Państwo tutaj.

Jeżeli Państwa zgłoszenie dotyczy aplikacji Lidl Plus, zastosowanie znajduje także polityka prywatności aplikacji.

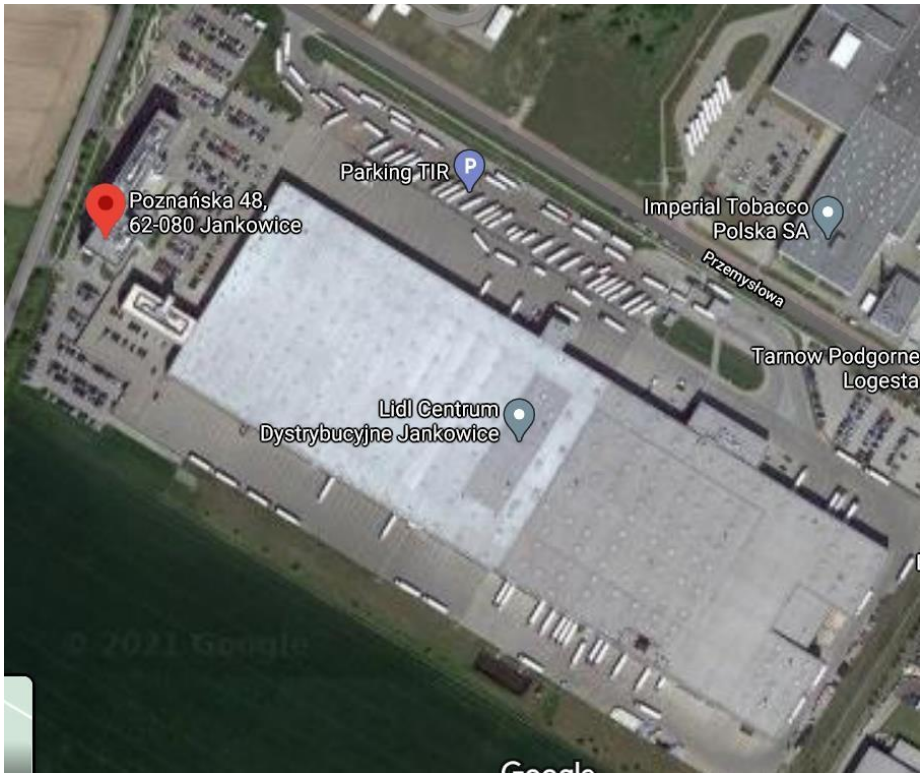
WYŚLIJ

Rys. 7. Formularz kontaktowy (zrzut ekranu – obsluga-klienta.lidl.pl).

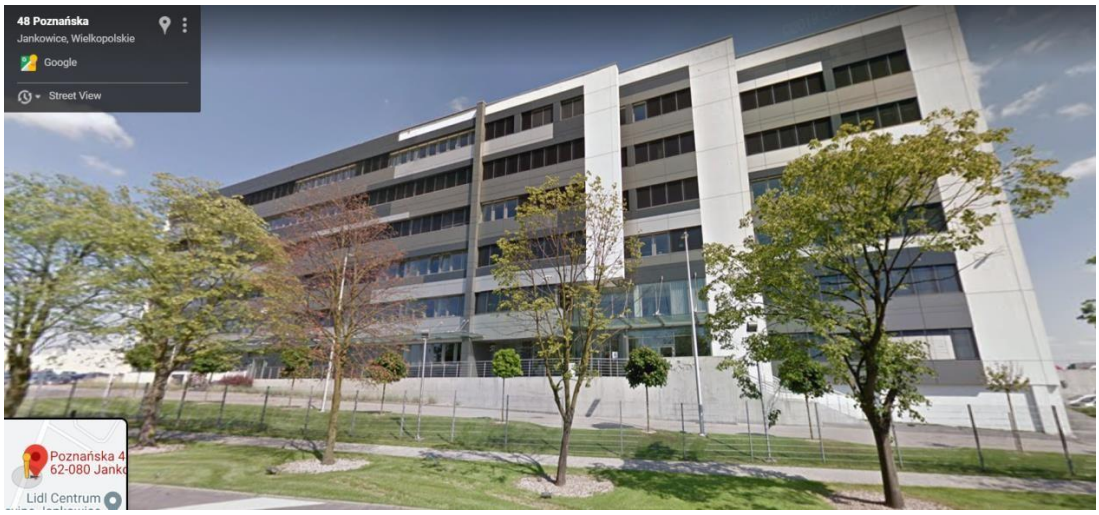
Siedziba Lidl Polska sp. z o.o. znajduje się na ul. Poznańskiej 48, Jankowice, 62-080 Tarnowo Podgórne, Polska. Adres siedziby można również sprawdzić na Google Maps, ponieważ został on podpisany jako „Lidl Centrum Dystrybucyjne Jankowice".



Rys. 8. Miejsce siedziby głównej Lidl w Polsce (zrzut ekranu – Google Maps).



Rys. 9. Zdjęcie satelitarne siedziby głównej Lidl w Polsce (zrzut ekranu – Google Maps).



Rys. 10. Obraz Street View siedziby głównej Lidl w Polsce (zrzut ekranu – Google Maps).

3. Serwery DNS obsługujące domenę.

Dzięki stronie who.is uzyskujemy potrzebne informacje, a mianowicie: adresy IP, nazwy serwerów DNS oraz informacje kontaktowe. Dowiadujemy się, że domena powstała w 2000 r. i wykorzystuje serwery Akami. Na załączonym zrzucie ekranu zaznaczona została również rubryka (REGISTAR) pod którą znajdziemy nazwę, lokalizację oraz dane kontaktowe firmy hostującej.

https://who.is/

```
DOMAIN NAME:            lidl.pl
registrant type:        organization
nameservers:            ns1-211.akam.net.
                        ns4-65.akam.net.
                        ns5-65.akam.net.
                        ns7-66.akam.net.
created:                2000.05.08 13:00:00
last modified:          2020.04.24 10:35:17
renewal date:           2021.05.07 14:00:00

option created:         2019.05.07 09:50:56
option expiration date:       2022.05.07 09:50:56

dnssec:                 Unsigned


REGISTRAR:
EuroDNS S.A.
21, rue Léon Laval
L-3372 Leudelange
+352 26 37 25 25
support@support.eurodns.com
www.eurodns.com
```

Rys. 11. Wyniki sprawdzenia domeny (zrzut ekranu – who.is).

DNS Records for lidl.pl

Hostname	Type	TTL	Priority	Content
lidl.pl	SOA	21599		ns1-211.akam.net hostmaster@akamai.com 1562059790 43200 7200 604800 3600
lidl.pl	NS	21599		ns4-65.akam.net
lidl.pl	NS	21599		ns1-211.akam.net
lidl.pl	NS	21599		ns5-65.akam.net
lidl.pl	NS	21599		ns7-66.akam.net
lidl.pl	A	19		104.127.81.70
lidl.pl	MX	3599	10	mail9.enc99-int.com
lidl.pl	MX	3599	20	mail3.enc99-int.com
lidl.pl	MX	3599	10	mail14.mail.schwarz
lidl.pl	MX	3599	10	mail10.enc99-int.com
lidl.pl	MX	3599	10	mail13.mail.schwarz
www.lidl.pl	A	19		104.127.81.70
www.lidl.pl	CNAME	369		lidl.pl.edgekey.net

Rys. 12. Raport szczegółowy DNS (zrzut ekranu – who.is).

https://urlscan.io/domain/lidl.pl

DNS records

A	23.196.200.179 (TTL: 19)
MX	mail9.enc99-int.com (Priority: 10)
MX	mail14.mail.schwarz (Priority: 10)
MX	mail13.mail.schwarz (Priority: 10)
MX	mail10.enc99-int.com (Priority: 10)
MX	mail3.enc99-int.com (Priority: 20)
NS	ns4-65.akam.net
NS	ns7-66.akam.net
NS	ns1-211.akam.net
NS	ns5-65.akam.net
TXT	swisssign-check=BEsKByaU5nacq19Jsc2cIOdsBaIkemXIuCiS64UZkZ
TXT	onetrust-domain-verification=e1183616e82b48c0afff655d6bef4805
TXT	facebook-domain-verification=fq8y0nssztb0ubpb383wnneoshs7dh
TXT	adobe-idp-site-verification=180da7a190fa4e0d92b513ceb07c05737d8dc50f521fcfd82319bd6a52116153
TXT	teamviewer-sso-verification=54e56f88cd134c04936e7c2b9a7c5dc9
TXT	webexdomainverification.4C675B8B74C0B136E053AB06FC0A3F65=0167c9e4-b7c7-498a-8f2e-05c2134bfede
TXT	v=spf1 mx ip4:185.49.148.16 include:_spfil1.mail.schwarz ?all
TXT	adobe-sign-verification=9b971b4430a524bb9ef5b9db2dc1d128
TXT	MS=ms27696417
TXT	google-site-verification=OD2UfXtWLyDs1cWChiOdyhDItUlCs2qrbztA6W1hcPY
TXT	apple-domain-verification=Y4oNGP3MQQr17Pb4
TXT	ciscocidomainverification=64d9ec5a1772c02b894889524b86d6a9a1eefbf6b856d018880b1ef2d2c5da55
SOA	ns1-211.akam.net hostmaster: hostmaster.akamai.com / serial: 1562059790 / refresh: 43200 / retry: 7200 / expire: 604800 / minttl: 3600 /

Rys. 13. Raport szczegółowy DNS (zrzut ekranu – urlscan.io).

https://www.robtex.com/

General	
FQDN	lidl.pl
Host Name	
Domain Name	lidl.pl
Registry	pl
TLD	pl
DNS	
IP numbers	23.47.141.152 23.77.141.142 23.196.104.125 23.204.54.79 23.212.30.142 23.223.183.157 104.82.115.153 104.116.39.184 184.85.129.222
Name servers	ns1-211.**akam**.net ns4-65.**akam**.net ns5-65.**akam**.net ns7-66.**akam**.net
Mail servers	mail10.**enc99-int**.com mail3.**enc99-int**.com mail9.**enc99-int**.com mail13.**mail**.schwarz mail14.**mail**.schwarz

Rys. 14. Wyniki sprawdzenia domeny (zrzut ekranu – robtex.com).

https://dns.pl/whois

Nazwa domeny	lidl.pl
Stan	Aktywna w DNS [REGISTERED]
Utworzona	2000.05.08 13:00:00
Ostatnia modyfikacja	2020.04.24 10:35:17
Koniec okresu rozliczeniowego	2021.05.07 14:00:00
Nazwy serwerów	ns1-211.akam.net ns4-65.akam.net ns5-65.akam.net ns7-66.akam.net
Abonent	Department Trademark Lidl Stiftung u. Co. KG Stiftsbergstr. 1 74167 Neckarsulm, DE +49.713294295354 Typ abonenta: organizacja Ostatnia modyfikacja: 2010.10.18 10:45:32
Rejestrator	EuroDNS S.A. 21, rue Léon Laval L-3372 Leudelange +352 26 37 25 25 support@support.eurodns.com www.eurodns.com
Opcja	Utworzona: 2019.05.07 09:50:56 Wygasa: 2022.05.07 09:50:56

Rys. 15. Wyniki sprawdzenia domeny (zrzut ekranu – dns.pl).

https://www.whois.com/whois/lidl.pl

lidl.pl

Updated 3 seconds ago

```
DOMAIN NAME:            lidl.pl
registrant type:        organization
nameservers:            ns1-211.akam.net.
                        ns4-65.akam.net.
                        ns5-65.akam.net.
                        ns7-66.akam.net.
created:                2000.05.08 13:00:00
last modified:          2020.04.24 10:35:17
renewal date:           2021.05.07 14:00:00

option created:         2019.05.07 09:50:56
option expiration date:       2022.05.07 09:50:56

dnssec:                 Unsigned


REGISTRAR:
EuroDNS S.A.
21, rue Léon Laval
L-3372 Leudelange
+352 26 37 25 25
support@support.eurodns.com
www.eurodns.com

WHOIS database responses: https://dns.pl/en/whois

WHOIS displays data with a delay not exceeding 15 minutes in relation to the
```

Rys. 16. Wyniki sprawdzenia domeny (zrzut ekranu – whois.com).

https://www.virustotal.com/gui/

Categories

Comodo Valkyrie Verdict	mobile communications
Forcepoint ThreatSeeker	business and economy
sophos	online shopping

Popularity Ranks

Rank	Value	Ingestion Time
Majestic	126610	2021-02-03 15:36:06
Statvoo	21916	2021-02-03 15:36:03
Alexa	21916	2021-02-03 15:36:02
Cisco Umbrella	902434	2021-01-26 15:57:38
Quantcast	215032	2020-03-31 15:36:07

Last DNS Records

	Record type	TTL	Value
	A	19	104.82.113.177
+	MX	3599	mail9.enc99-int.com
+	MX	3599	mail14.mail.schwarz
+	MX	3599	mail3.enc99-int.com
+	MX	3599	mail10.enc99-int.com
+	MX	3599	mail13.mail.schwarz
	NS	21599	ns1-211.akam.net
	NS	21599	ns4-65.akam.net
	NS	21599	ns7-66.akam.net
	NS	21599	ns5-65.akam.net

Rys. 17. Wyniki sprawdzenia domeny (zrzut ekranu – virustotal.com).

https://domainwat.ch/

lidl.pl

Search on other sites

(None) (None) (None)

(None)

(None)

(None)

DOMAIN NAME: lidl.pl

registrant type: organization

nameservers: ns1-211.akam.net.

ns4-65.akam.net.

ns5-65.akam.net.

ns7-66.akam.net.

created: 2000.05.08 13:00:00

last modified: 2020.04.24 10:35:17

renewal date: 2021.05.07 14:00:00

2020/11/18 17:51:09

option created: 2019.05.07 09:50:56

option expiration date: 2022.05.07 09:50:56

dnssec: Unsigned

REGISTRAR:

EuroDNS S.A.

21, rue Léon Laval

L-3372 Leudelange

DNS Records

2020/12/23 02:15:28
2020/12/04 13:49:32
2020/10/26 01:57:19
2020/10/21 17:31:49
2020/10/08 15:06:21
2020/09/21 05:55:24
2020/09/18 01:24:53
2020/08/20 00:46:27
2020/08/06 13:33:43
2020/07/23 07:05:55
2020/07/08 21:16:54
2020/07/07 09:17:36
2020/06/24 21:19:03
2020/06/23 15:24:41
2020/06/23 05:12:14
2020/06/22 10:13:06
2020/06/20 08:22:37
2020/06/10 10:31:02
2020/06/09 13:31:10
2020/06/08 02:46:35
2020/06/07 14:01:21
2020/06/06 00:51:44
2020/04/08 13:36:50
2020/04/07 10:56:15
2020/04/03 09:11:19
2020/04/01 16:10:32
2020/02/08 13:37:15

Type	Hostname	TTL	Content
A	lidl.pl	19	104.103.109.9
MX	lidl.pl	3599	10 mail13.mail.schwarz
MX	lidl.pl	3599	20 mail3.enc99-int.com
MX	lidl.pl	3599	10 mail9.enc99-int.com
MX	lidl.pl	3599	10 mail10.enc99-int.com

Rys. 18. Wyniki sprawdzenia domeny (zrzut ekranu – domainwatch.ch).

Można zauważyć że używane są serwery firmy Akami.Serwery te korzystają z technologii DNS Anycast, która polega na połączeniu użytkownika z najbliższym punktem Akami co skutkuje najszybszym możliwym czasem ładowania się strony. Warto zauważyć, że dzięki serwerom Akami ukrywane są serwery i uniemożliwiany jest dostęp do strony dla osób mogącym mieć na nią zły wpływ, czyli tzw. niepożądanym użytkownikom.

Cloud-based DNS for improved performance, availability, and resiliency against DDoS attacks.

Akamai's Edge DNS is a cloud-based solution that delivers 24/7 DNS availability, improves DNS responsiveness, and ensures DNS security by fending off the largest DDoS attacks. Built on a globally distributed network, Edge DNS can be implemented as a primary or secondary DNS service.

Edge DNS promotes DNS security by providing a highly scalable platform that has enough capacity to absorb the largest DDoS attacks while also responding to legitimate user requests, enabling you to maintain availability and performance even while under attack. An optional add-on, Akamai DNSSEC, provides additional DNS security by helping to prevent DNS forgery and manipulation.

Rys. 19. Odpis działania serwerów Akami (zrzut ekranu – oficjalna strona Akami).

Adresy uzyskane przez wykonane skany nie są faktycznymi adresami strony lidl.pl. W celu sprawdzenia czy podane stwierdzenie jest prawdą, postaram się sprawdzić dwa różne adresy IP odpowiadające badanej witrynie w różnych narzędziach.

Jako pierwsze użyłem narzędzia sitereport.netcraft.pl. Uzyskany rezultat po wpisaniu „lidl.pl”.

Site	http://lidl.pl
Netblock Owner	Akamai Technologies, Inc.
Hosting company	Akamai Technologies
Hosting country	US
IPv4 address	96.16.229.174 (VirusTotal)

Rys. 20. Uzyskany adres IP ver.1 (zrzut ekranu – sitereport.netcraft.pl).

Jako odpowiedź przeglądarki otrzymujemy raport o błędzie:

Niezabezpieczona | 96.16.229.174

Invalid URL

The requested URL "[no URL]", is invalid.

Reference #9.d47032b8.1611524607.8620fd1

Rys. 21. Nieudana próba (zrzut ekranu – Google Chrome).

Jako drugi sposób uzyskania IP wykorzystałem konsolę systemu Windows (cmd). Za pomocą polecenia tracert oraz wpisania adresu strony uzyskujemy zaznaczony kolorem adres IP.

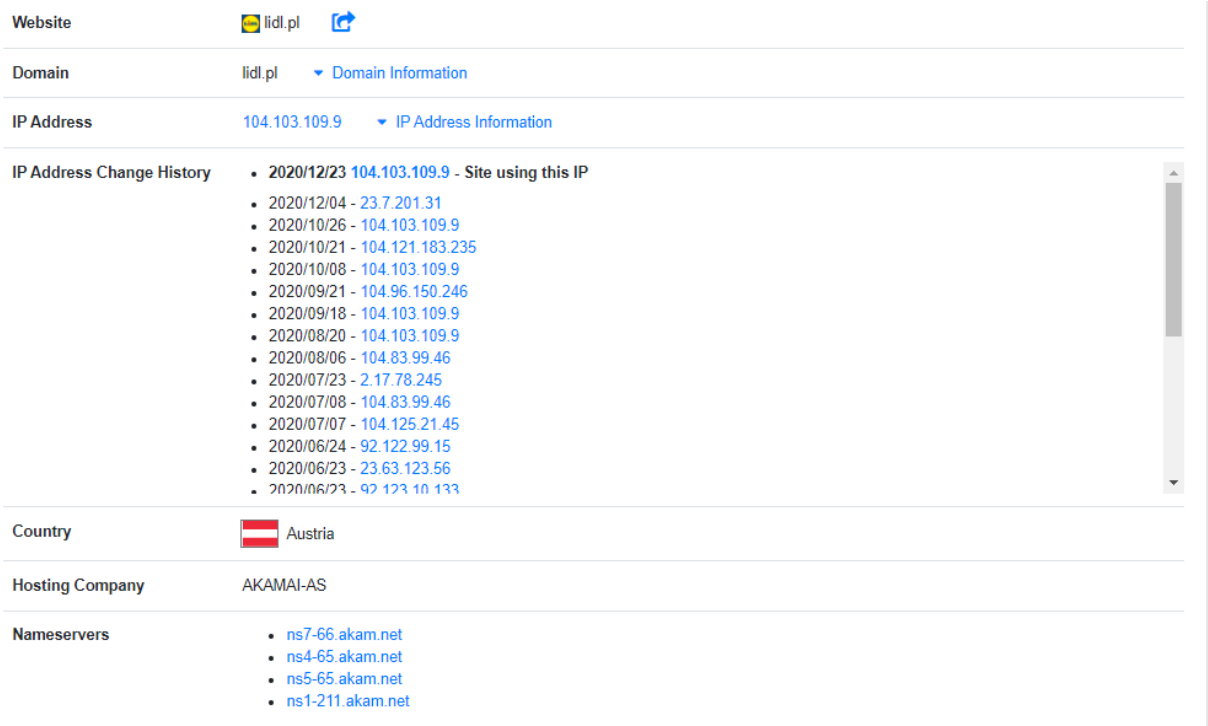
Wiersz polecenia

```
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\Szymon>tracert lidl.pl

Tracing route to lidl.pl [104.87.177.235]
over a maximum of 30 hops:
```

Rys. 22. Uzyskany adres IP ver.2 (zrzut ekranu – cmd).

Również w tym przypadku sprawa wygląda podobnie – prawie tak samo.

Rys. 23. Nieudana próba (zrzut ekranu – Google Chrome).



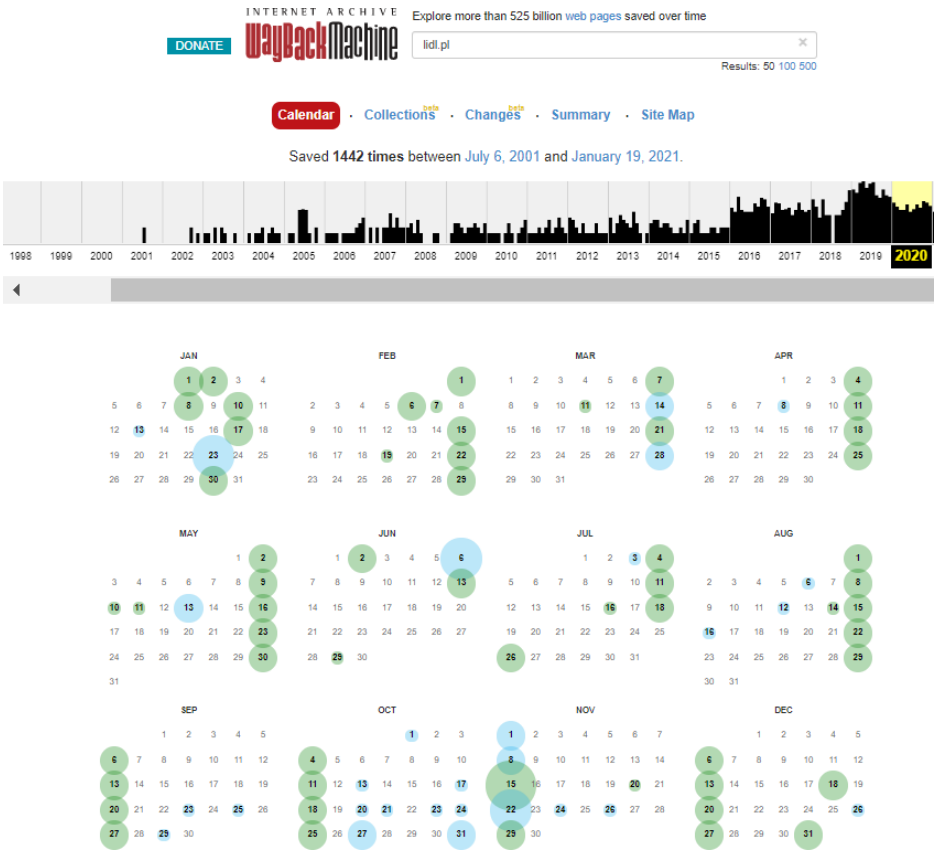
Rys. 24. Informacje o witrynie (zrzut ekranu – domainwatch.ch).

Po wpisaniu każdego ukazanego adresu IP (sprawdzane w 3 przypadkach), nie zostajemy przekierowani na właściwą stronę lidl.pl. Adresy IP za każdym razem są różne. Zawsze ukazuje się ten sam błąd, który został ukazany na rysunkach powyżej. Na powyższym rys. została ukazana historia zmiany adresu IP w określonych dniach/miesiącach. Adresy uzyskane przez wykonane skany nie są faktycznymi adresami strony lidl.pl.

4. <u>Ogólne dane dotyczące witryny domeny.</u>

Z załączonego zrzutu możemy zauważyć, że ostatnia modyfikacja na stronie została przeprowadzona dnia 24.04.2020 r. o godzinie 10:35. Uzyskujemy tu również nazwy serwerów DNS.

Dzięki wykorzystaniu WayBack Machine, uzyskujemy informacje odnośnie częstotliwości zmian (modyfikacji) wprowadzanych na stronie

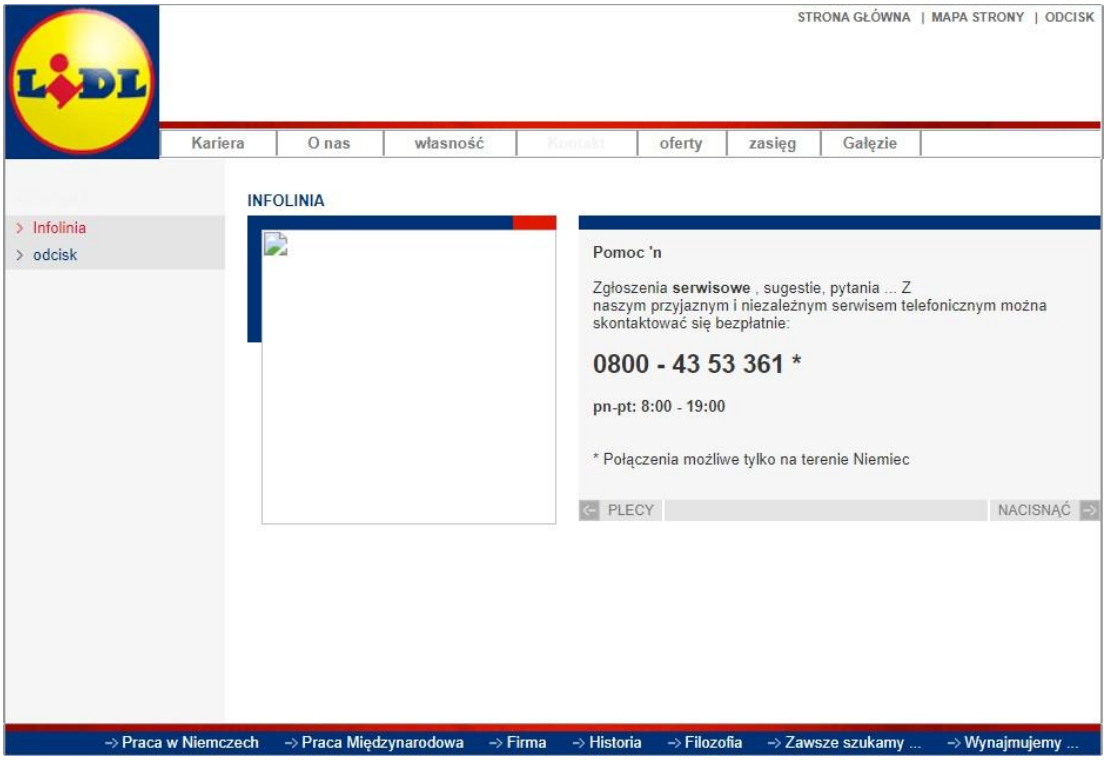


Rys. 25. Modyfikacje w roku 2020 (zrzut ekranu – WayBack Machine)

W celu porównania rozwoju strony internetowej poniżej zamieszczona jest witryna lidl.pl (wtedy http://www.karriere-bei-lidl.de/) z roku 2002.

Rys. 26. Witryna lidl.pl, rok 2002 (zrzut ekranu – WayBack Machine).

Dzięki temu możemy zauważyć, że strona głównie prezentowała treści związane z podjęciem pracy w sieci sklepów dyskontowych, ale również znajdziemy tam dane kontaktowe. Po wejściu w tę zakładkę i przetłumaczeniu strony otrzymujemy następujące informacje:

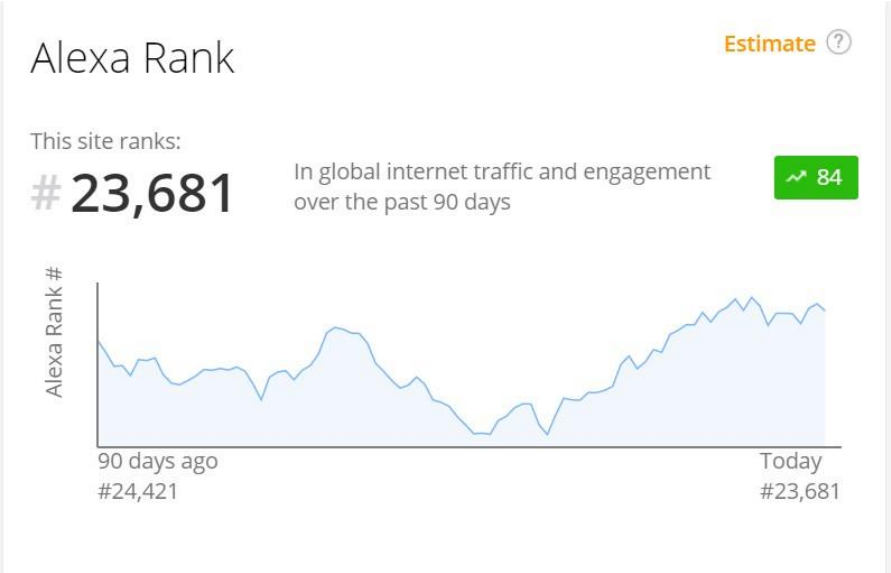


Rys. 27. Witryna lidl.pl, rok 2002, sekcja kontakt(zrzut ekranu – WayBack Machine).

Rys. 19. Portal obsługi klienta (zrzut ekranu – lid.pl).

Dla porównania z rokiem 2002 został przedstawiony wygląd aktualnego okna obsługi klienta. Możemy zauważyć większe zaawansowanie w aktualnej rubryce niż w całości strony z tamtego okresu.

Popularność strony została przebadana za pomocą strony alexa.com i przedstawia się następująco:



Rys. 28. https://www.alexa.com/siteinfo/lidl.pl (zrzut ekranu – alexa.com).

Ranking popularności względem strony virustotal.com:

Popularity Ranks

Rank	Value	Ingestion Time
Majestic	126610	2021-02-03 15:36:06
Statvoo	21916	2021-02-03 15:36:03
Alexa	21916	2021-02-03 15:36:02
Cisco Umbrella	902434	2021-01-26 15:57:38
Quantcast	215032	2020-03-31 15:36:07

Rys. 29. Ranking popularności (zrzut ekranu – virustotal.com).

Z podanego wykresu możemy zauważyć, że strona nie ma ani tendencji spadkowej ani wzrostowej. Strona notuje wzrosty popularności, na mniej więcej podobnym poziomie co spadki. Natomiast ranking popularności ze strony virustotal.com wskazuje dość różne wyniki. Moim zdaniem jest to spowodowane zmieniającą się ofertą artykułów oferowanym w sklepie internetowym. W ciągu 90 dni strona wniosła się na szczeblach rankingu z 24,421 na 23,681. Możemy zauważyć wzrost zainteresowania. Może być to spowodowane sytuacją epidemiczną i chętniej wybieranymi zakupami internetowymi.

5. Struktura domeny.

Do sprawdzenia poddomen użyłem strony dnsdumpster.com. Skanowanie wykonałem za pomocą nazwy domeny, a nie za pomocą IP. Po wykonaniu skanu za pomocą nazwy uzyskałem następujące rezultaty:

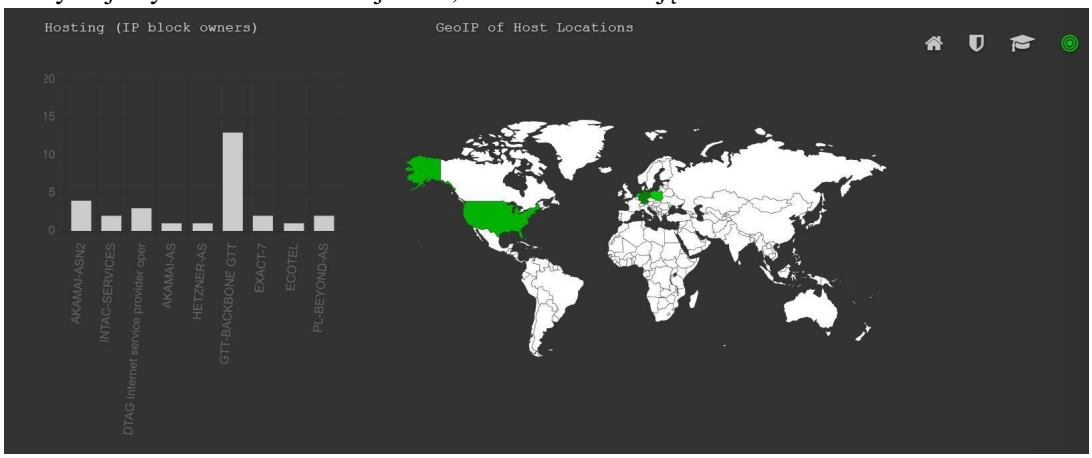
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

lidl.pl HTTP: AkamaiGHost HTTPS: AkamaiGHost	23.10.89.89 a23-10-89- 89.deploy.static.akamaitechnologies.com	AKAMAI-AS United States
gazetka.lidl.pl HTTP: Apache/2.4.25 (Debian) SSH: SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7 HTTP TECH: Debian Apache,2.4.25	136.243.111.164 images.fashionmodeldirectory.com	HETZNER-AS Germany
promocje.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
casting.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
marki.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
marki.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
ryneczek.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
rzeznik.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
pikok.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
email.lidl.pl	136.147.129.27 reply-mx.s7.exacttarget.com	EXACT-7 United States
mta.email.lidl.pl	13.111.13.239 mta.email.lidl.pl	EXACT-7 United States
ssl.lidl.pl HTTPS: Lotus-Domino	213.39.49.15	GTT-BACKBONE GTT Germany

bio.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
newsletter.lidl.pl HTTP: Apache HTTPS: Apache	62.27.38.101 fagms.net	ECOTEL Germany
pilos.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
newsletters.lidl.pl HTTP: Apache HTTPS: Apache HTTPS TECH: Laravel	195.81.83.99	GTT-BACKBONE GTT Germany
toujours.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
crivit.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
lupilu.lidl.pl HTTP: Apache/2.4.34 (Red Hat) OpenSSL/1.0.2k-fips HTTP TECH: Apache,2.4.34	195.81.83.97	GTT-BACKBONE GTT Germany
faktury.lidl.pl HTTP: Microsoft-HTTPAPI/2.0 HTTPS: Microsoft-HTTPAPI/2.0	185.23.20.131 ip-185-23-20-131.beyond.pl	PL-BEYOND-AS Poland
www.faktury.lidl.pl HTTP: Microsoft-HTTPAPI/2.0 HTTPS: Microsoft-HTTPAPI/2.0	185.23.20.131 ip-185-23-20-131.beyond.pl	PL-BEYOND-AS Poland

Rys. 30. Poddomeny wraz z IP (zrzut ekranu – https://dnsdumpster.com/).

Uzyskany wynik prezentuje nazwy poddomen, jest ich 20. Możemy zauważyć powtarzające się domeny (np. dwie ostatnie). Za pomocą tego skanowania otrzymujemy również informacje o IP, a także lokalizację.



Rys. 31. Lokalizacje (zrzut ekranu –https://dnsdumpster.com/).

Na powyższym rysunku możemy zobaczyć lokalizację danych hostów rozmieszczonych na mapie świata. Łatwo zauważyć, że najwięcej ich znajduje się w Niemczech (co jest zrozumiałe, z racji tego że jest to firma która powstałą w tym kraju).

Lista poddomen uzyskanych za pomocą strony virustotal.com

Subdomains

webcontent.lidl.pl	104.88.206.154	104.88.206.148	23.33.85.33	...
www.lidl.pl	96.17.112.202	23.79.208.152	23.204.21.155	...
spedycja.lidl.pl	185.49.148.236			
faktury.lidl.pl	185.23.20.131			
kariera.lidl.pl	23.65.255.207	23.4.102.239	23.6.157.160	...
kimjestesmy.lidl.pl	23.65.242.130	23.5.240.41	23.222.140.118	...
news.lidl.pl	93.191.162.150			
service.lidl.pl	93.191.162.150			
obsluga-klienta.lidl.pl	13.109.130.51	85.222.154.12	85.222.154.140	...
store.lidl.pl	213.144.6.110			
swasc.lidl.pl	34.227.41.189	3.219.249.186	54.90.190.103	...
email.lidl.pl	136.147.129.27			
casting.lidl.pl	195.81.83.97			
rezerwuj.lidl.pl	51.138.116.1	13.109.215.223	85.222.145.140	...
rzeznik.lidl.pl	195.81.83.97	195.81.83.74		
poc.lidl.pl	80.92.65.53			
marki.lidl.pl	195.81.83.97	213.39.15.20		
cncauthuat.lidl.pl	77.87.187.36			
cncauthprod.lidl.pl	77.87.187.36			
cncauthdev.lidl.pl	77.87.187.36			
ezakupy.lidl.pl	185.49.148.213			
pilos.lidl.pl	195.81.83.97	195.81.83.74		
pikok.lidl.pl	213.39.15.20			
toujours.lidl.pl	213.39.15.17			
promocje.lidl.pl	213.39.15.17			
lupilu.lidl.pl	195.81.83.74			
newsletter.lidl.pl	62.27.38.101			
ryneczek.lidl.pl	195.81.83.74			
crivit.lidl.pl	213.39.15.36			
ssl.lidl.pl	213.39.49.15			
bio.lidl.pl	195.81.83.74			
gazetka.lidl.pl	46.4.95.235	148.251.69.139	144.76.91.169	...
l.newsletter.lidl.pl	62.27.116.25			
www.swiatryb.lidl.pl	188.165.228.85			
nieruchomosci.lidl.pl	66.198.26.50	23.63.227.208	66.198.26.56	...

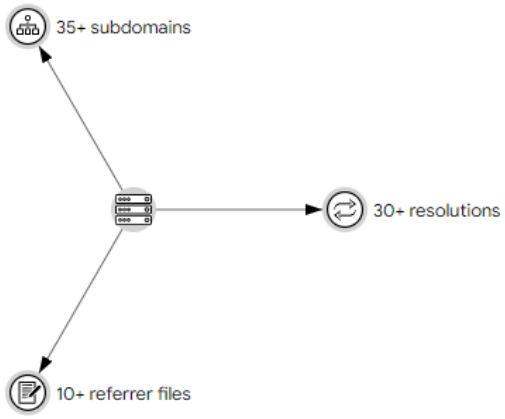
Passive DNS Replication

Date resolved	IP
2021-02-03	23.51.173.39
2021-01-29	104.127.149.2
2021-01-29	23.222.137.213
2021-01-25	184.85.25.119
2021-01-21	104.122.157.142
2021-01-17	104.100.149.95
2021-01-10	23.67.126.92
2021-01-08	184.29.166.249
2020-12-15	2.20.236.238
2020-12-12	23.199.188.148
2020-12-10	23.36.86.14
2020-12-10	23.60.54.94
2020-12-07	23.61.183.124
2020-12-03	104.79.153.202
2020-11-22	23.78.68.149
2020-11-20	23.3.171.90
2020-11-19	23.199.31.57
2020-11-17	104.105.235.172
2020-11-15	104.97.111.190
2020-11-11	23.7.140.251
2020-10-01	23.65.252.153

Historical SSL Certificates

	First seen	Subject	Thumbprint
+	2020-06-09	retail.lidl	88a2621d941491174acf388e33832edfbfcd9b0a
+	2019-08-13	retail.lidl	efd560df1c583d9eed6eb097d545dea9b9f4d448

Graph Summary



Rys. 32. Lista poddomen (zrzut ekranu –virustotal.com).

Categories

Forcepoint ThreatSeeker	information technology

HTTP Response

Final URL

http://96.17.112.202/

Serving IP Address

96.17.112.202

Status Code

400

Body Length

208.00 B

Body SHA-256

5f0aae1ea2fdd524513d04030a5c9ae27dfae0f5dc6bf302a94f4f0be5fc5450

Headers

connection	close
content-length	208
content-type	text/html
date	Thu, 04 Feb 2021 15:23:57 GMT
expires	Thu, 04 Feb 2021 15:23:57 GMT
mime-version	1.0

Rys. 33. Skan za pomocą adresu IP (zrzut ekranu –virustotal.com).

Za pomocą wykonanego skanu otrzymujemy listę aż 35 poddomen. Przy każdym widnieje odpowiadający jej adres IP. Niestety skan za wykonany za pomocą adresu IP nie przyniósł wielu rezultatów. Nie uzyskujemy żadnych szczegółowych informacji, adres IP za każdym razem jest inny. W tym przypadku skanowany adres IP to : 96.17.112.202.

6. <u>Wykorzystywane systemy operacyjne, usługi sieciowe i aplikacje realizujące te usługi.</u>

Przy realizacji tego punktu używałem strony netcraf.com. Otrzymane informacje:

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.142.92	Linux	AkamaiGHost	20-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.142.78	Linux	AkamaiGHost	19-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.216.73	Linux	AkamaiGHost	18-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.142.78	Linux	AkamaiGHost	17-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.216.73	Linux	AkamaiGHost	16-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.142.92	Linux	AkamaiGHost	14-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.123.142	Linux	AkamaiGHost	9-Apr-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.252.97	Linux	AkamaiGHost	8-Apr-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.123.142	Linux	AkamaiGHost	6-Apr-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.252.97	Linux	AkamaiGHost	2-Apr-2020

Rys. 34. Systemy operacyjne (zrzut ekranu – netcraf.com)

Następnie wykonałem skan za pomocą witryny **shodan.io** i wkleiłem jeden z serwerów.

20.54.140.80
Microsoft Azure
Added on 2021-01-24 02:28:55 GMT
Netherlands, Amsterdam
cloud

SSL Certificate
Issued By:
|- Common Name: SwissSign EV Gold CA 2014 - G22
|- Organization: SwissSign AG
Issued To:
|- Common Name: accounts.lidl.com
|- Organization: Lidl Stiftung & Co. KG

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 200 OK
Date: Sun, 24 Jan 2021 02:28:55 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Request-Context: appId=cid-v1:be7cc2bc-1192-492b-b0fd-f317cfe7e5a5
Strict-Transport-Security: max-age=10886400; includeSubDomains; preload
Content-Se...
```

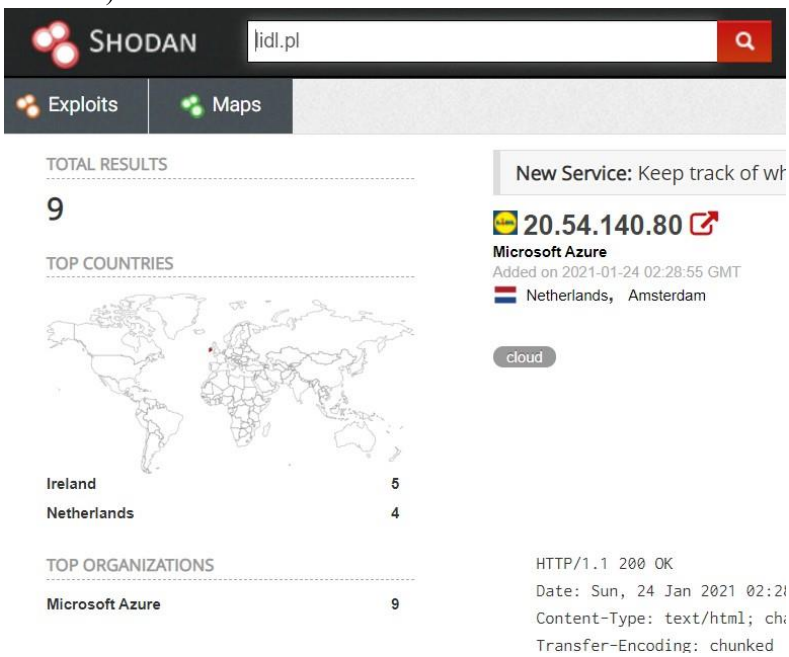
Services

80
tcp
http

```
HTTP/1.1 301 Moved Permanently
Server: Microsoft-Azure-Application-Gateway/v2
Date: Tue, 19 Jan 2021 23:23:25 GMT
Content-Type: text/html
Content-Length: 195
Connection: keep-alive
Location: https://51.104.185.154/
```

Rys. 35. Systemy operacyjne (zrzut ekranu – shodan.io)

Z pierwszego skanu możemy wywnioskować, że wszystkie serwery działają na Linuxie. Drugi skan zaś pokazał (w tym przypadku na przykładzie jednego z nich), ze systemem operacyjnym jest Microsoft Windows (wiemy to dzięki informacji Server: „Microsoft Azure”).



Rys. 36. Systemy operacyjne (zrzut ekranu – shodan.io)

Za pomocą shodan.io otrzymujemy informację, że każdy serwery działa na systemie Microsoft Windows. W tym punkcie otrzymane informacje są sprzeczne i nie wiem jak je analizować.

Nie jestem w stanie stwierdzić jaki system operacyjny mają podane serwery. Na pierwszym screenie (skan wykonany netcraft’em)jest to Linux, zaś na kolejnych widzimy obecność Microsoft Azure, więc musi to być Windows. Na zrzutach zostały również przedstawione adresy IP i rozlokowanie na mapie. Możemy zauważyć, że używanym językiem jest głównie html/sql.

7. Wykorzystane technologie informatyczne.

Strona wygląda na dość zaawansowana technologicznie. Mamy wiele możliwości wyboru i niektóre opcje dostępne są dopiero po zalogowaniu. Informacje o użytych technologiach zdobyłem za pomocą witryny netcraft.com.

Site Technology (fetched today)

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Varnish	An HTTP accelerator for web applications	www.investing.com, js.stripe.com, acdn.adnxs.com

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
XML	*No description*	www.hulu.com, www.pinterest.com, www.virustotal.com
SSL	A cryptographic protocol providing communication security over the Internet	

Rys. 37. Technologie informatyczne (zrzut ekranu – netcraft.com)

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
Asynchronous Javascript	*No description*	www.espn.com, www.deepl.com, www.roblox.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.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
Google Tag Manager	*No description*	www.digikala.com, www.booking.com, www.20minutes.fr
RequireJS	*No description*	www.geeksforgeeks.org, www.bankofamerica.com, www.chase.com

E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

Technology	Description	Popular sites using this technology
General Domain Holding	Loading temporary content under a domain name	www.apple.com, www.microsoft.com, www.amazon.in

Rys. 38. Technologie informatyczne (zrzut ekranu – netcraft.com)

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.ecosia.org, www.instagram.com, www.qwant.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	www.twitch.tv, www.linkedin.com, mail.google.com
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	web.whatsapp.com, accounts.google.com, teams.microsoft.com
Content Security Policy	Detect and mitigate attacks in the browser	mail.yahoo.com, e.mail.ru, discord.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	

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	

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.amazon.fr

Rys. 39. Technologie informatyczne (zrzut ekranu – netcraft.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
External	Styles defined within an external CSS file	www.binance.com, www.paypal.com, www.amazon.co.uk

Rys. 40. Technologie informatyczne (zrzut ekranu – netcraft.com)

The ports found on the targeted host

Port	State	Service	Product	Product Version	Risk Level
80	open	http	AkamaiGHost		INFO
443	open	https	AkamaiGHost		INFO

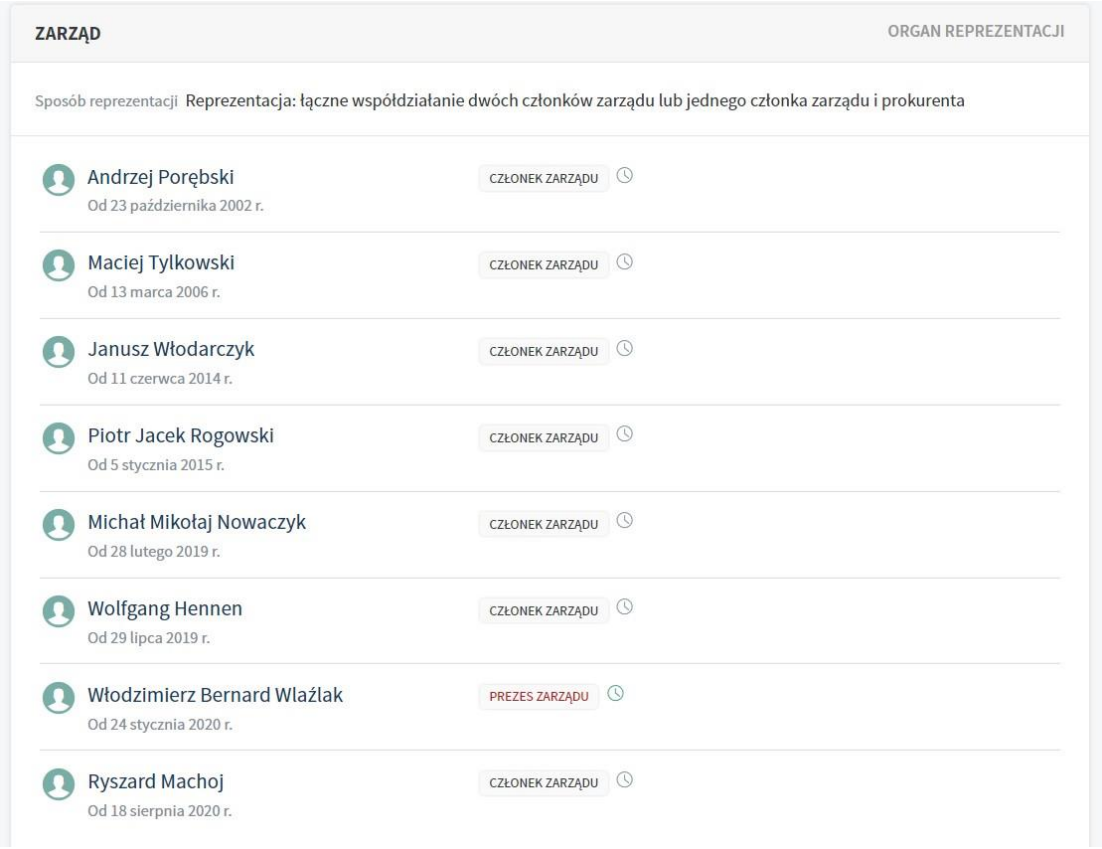
Rys. 41. Porty (zrzut ekranu – pentest-tool)

Dzięki witrynie netcraft i pentest-tools otrzymujemy dokładne dane na temat wykorzystanej technologii, portów a także jej/ich opis. Na zamieszczonych zrzutach możemy zobaczyć, że zostały użyte typowe technologie do tego typu stron (np. Google Tag Manager).

8. Pracownicy i osoby powiązane.

Niestety na stronie internetowej nie otrzymujemy informacji odnośnie pracowników, którzy działają na rzecz tej strony. Jest to opisane bardzo ogólnie i nie możliwe jest znalezienie imion i nazwisk, bądź adresów osób pracujących nad rozwojem i administracją tej strony. Natomiast jako, że Lidl jest jedną z największych firm na świecie otrzymujemy dużo informacji o zarządzie.

Od dnia 24 stycznia 2020 r. prezesem zarządu jest Włodzimierz Bernard Wlaźlak (członek zarządu od 12 grudnia 2019 r.). W skład zarządu wchodzą również: Andrzej Porębski, Maciej Tylkowski, Janusz Włodarczyk, Piotr Jacek Rogowski, Michał Mikołaj Nowaczyk, Wolfgang Hannen i Ryszard Machoj. Jedynym, a zarazem głównym wspólnikiem jest Lidl spółka z ograniczoną odpowiedzialnością (od 11 maja 2016 r.)



ZARZĄD | ORGAN REPREZENTACJI

Sposób reprezentacji Reprezentacja: łączne współdziałanie dwóch członków zarządu lub jednego członka zarządu i prokurenta

Andrzej Porębski Od 23 października 2002 r.	CZŁONEK ZARZĄDU
Maciej Tylkowski Od 13 marca 2006 r.	CZŁONEK ZARZĄDU
Janusz Włodarczyk Od 11 czerwca 2014 r.	CZŁONEK ZARZĄDU
Piotr Jacek Rogowski Od 5 stycznia 2015 r.	CZŁONEK ZARZĄDU
Michał Mikołaj Nowaczyk Od 28 lutego 2019 r.	CZŁONEK ZARZĄDU
Wolfgang Hennen Od 29 lipca 2019 r.	CZŁONEK ZARZĄDU
Włodzimierz Bernard Wlaźlak Od 24 stycznia 2020 r.	PREZES ZARZĄDU
Ryszard Machoj Od 18 sierpnia 2020 r.	CZŁONEK ZARZĄDU

Rys. 42. Członkowie zarządu (zrzut ekranu - rejestr.io).

WSPÓLNICY

LIDL SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Od 11 maja 2016 r.

Wartość udziałów 18,2 mln zł
Liczba udziałów 363200
Posiada całość akcji spółki TAK

Zobacz jeszcze 1 wpis historyczny

Rys. 43. Wspólnicy (zrzut ekranu - rejestr.io).

Z racji objętości projektu załączona została tylko część prokurentów

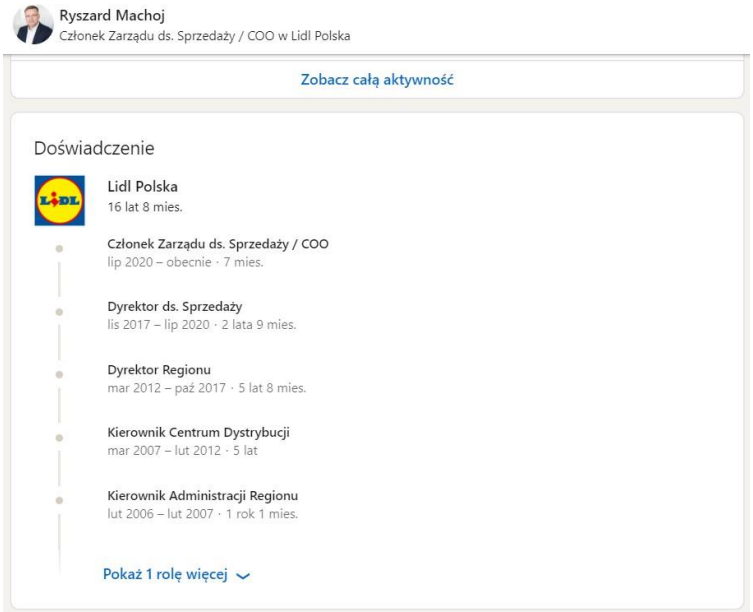
PROKURENCI

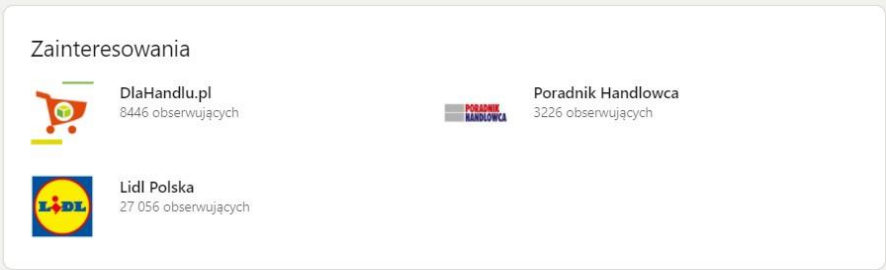
Dorota Jeziak Od 9 stycznia 2006 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Robert Michał Górny Od 9 stycznia 2006 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Maciej Marcinkowski Od 5 lipca 2013 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Jan Szymon Słowik Od 5 lipca 2013 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Piotr Andrzej Michaś Od 27 maja 2015 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Justyna Stefania Siekanko Od 24 listopada 2017 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Rafał Mielcarek Od 28 lutego 2019 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW
Przemysław Styperek Od 9 października 2019 r.	PROKURA ŁĄCZNA Z JEDNYM Z POZOSTAŁYCH PROKURENTÓW

Rys. 44. Część prokurentów (zrzut ekranu - rejestr.io).

Rys. 45. Powiązania zarządu oraz prokurentów (zrzut ekranu - rejestr.io).

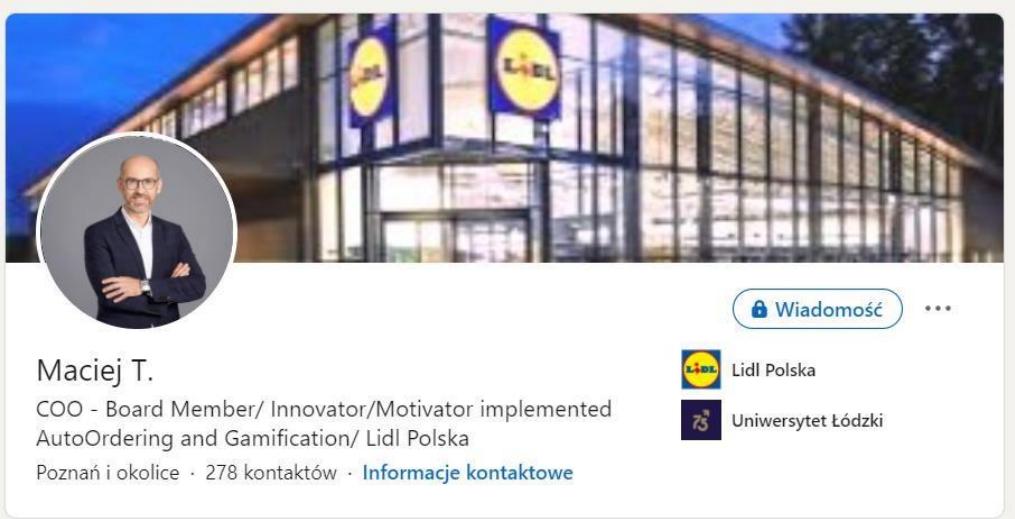
Ryszard Machoj – określony beneficjentem rzeczywistym (na stronie rejestr.io).

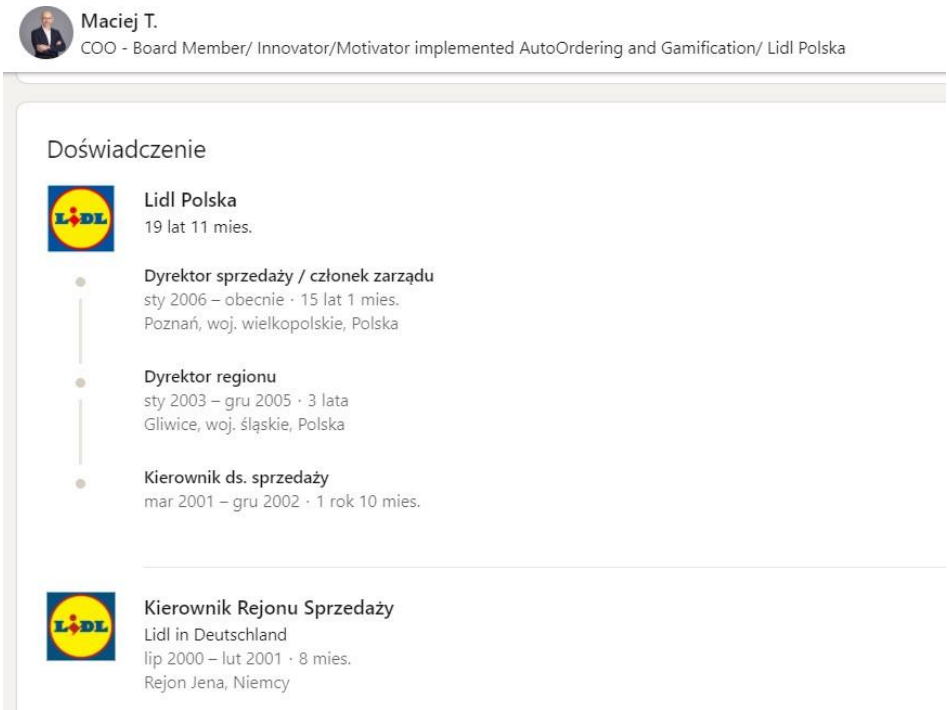


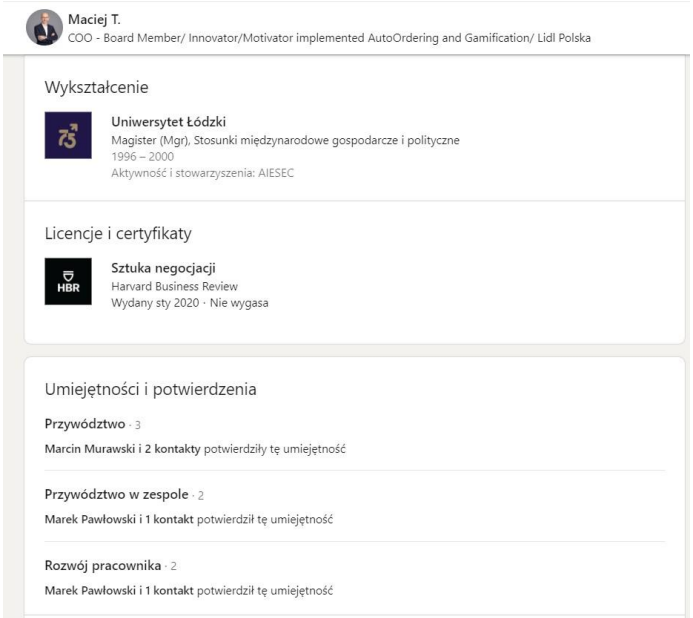


Rys. 46. Beneficjent - zarząd (zrzut ekranu – linkedin.com).

Maciej Tylkowski

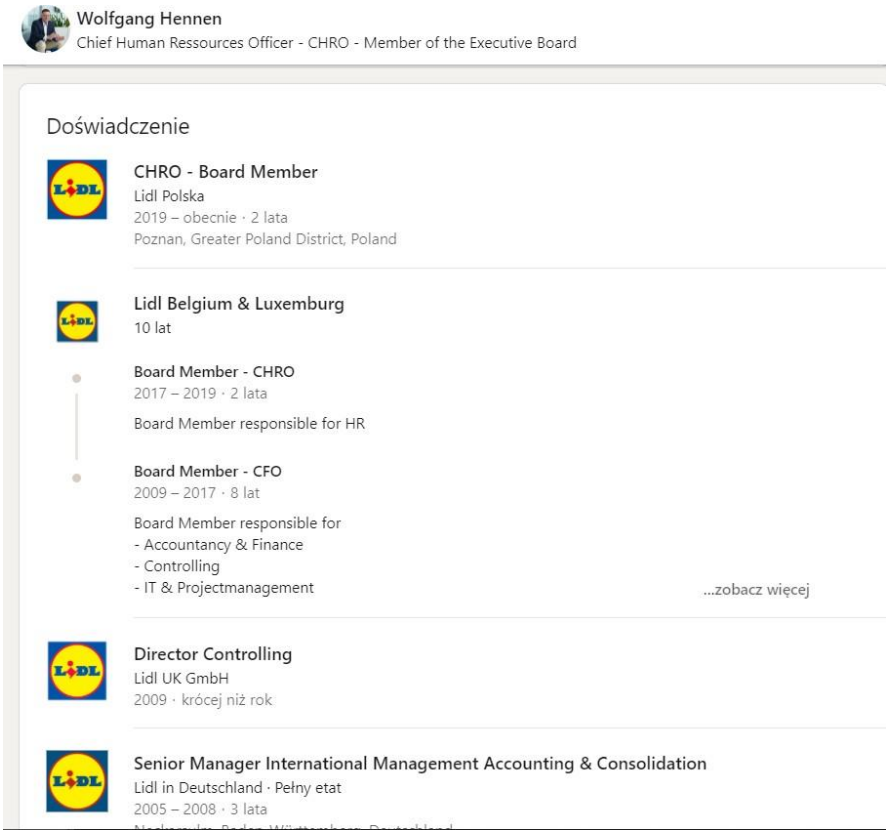


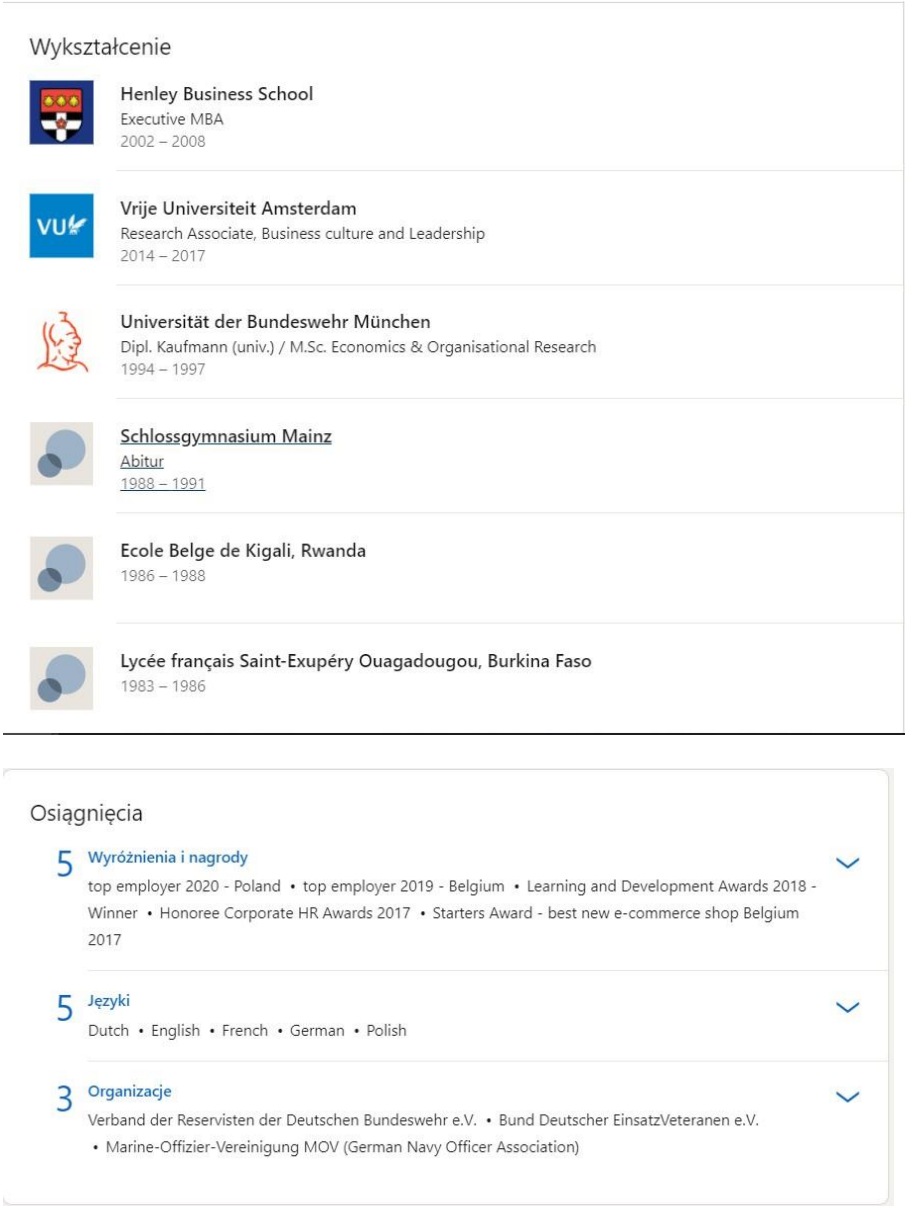




Rys. 47. Zarząd (zrzut ekranu – linkedin.com).

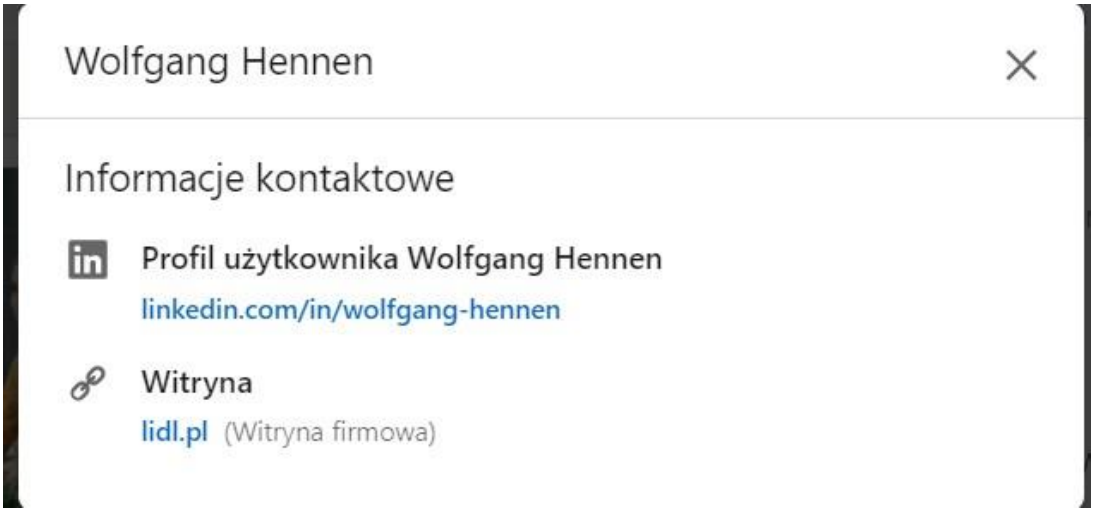
Wolfgang Hennen





Rys. 48. Zarząd (zrzut ekranu – linkedin.com).

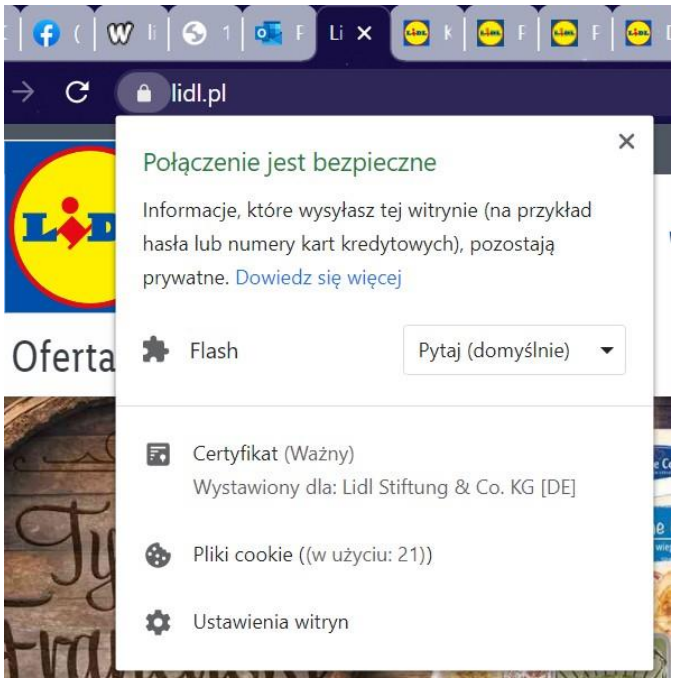
Niestety uzyskanie większej ilości informacji jest niemożliwe, po sprawdzeniu każdego członka zarządu, beneficjenta, a nawet prezesa nie jestem w stanie uzyskać większej ilości informacji niż wykształcenie, aktualna praca czy zainteresowania. Żadna ze sprawdzonych osób nie jest widoczna na Facebook'u ani na innym portalu społecznościowym niż linkedin.com.



Rys. 48. Zarząd - informacje (zrzut ekranu – linkedin.com).

Gdy sprawdzałem informacje otrzymywałem jedynie coś w stylu informacji zamieszczonych na zamieszczonych rysunkach. Wykonany został na przykładzie Wolfganga Hennen'a, ale sytuacja u każdej sprawdzanej osoby wygląda tak samo.

9. Bezpieczeństwo.



Rys. 49. Połączenie z witryną (zrzut ekranu – Google Chrome).

Na wyżej załączonym zrzucie możemy zauważyć ze połączenie jest bezpieczne i google suport nie wykazuje przeciwskazań korzystania z tej witryny. Certyfikat jest ważny, więc podawane dane zostaną tajne.

Następnie wykonałem skan za pomocą witryny virustotal.com:

ADMINUSLabs	Clean	AegisLab WebGuard	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	Armis	Clean
Artists Against 419	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Botvrij.eu	Clean
Certego	Clean	CINS Army	Clean
CLEAN MX	Clean	CMC Threat Intelligence	Clean
Comodo Site Inspector	Clean	Comodo Valkyrie Verdict	Clean
CRDF	Clean	CyberCrime	Clean
CyRadar	Clean	Cyren	Clean
desenmascara.me	Clean	DNS8	Clean

Rys. 50. Bezpieczeństwo (zrzut ekranu – virustotal.com).

Files Referring

Scanned	Detections	Type	Name
2020-06-16	0 / 69	Win32 EXE	palemoon-28.9.0.2.win64.installer.exe
2020-01-23	1 / 67	Win32 DLL	xul.dll
2020-08-07	38 / 69	Win32 DLL	srns.dll
2019-06-05	26 / 70	Win32 DLL	Smartbar.Resources.NetSeer.dll
2019-03-11	1 / 61	Office Open XML Spreadsheet	79408f6289700c7b47e2e81dcc05a436bf2c6e1db3e436173b348bcd08945c8c
2019-02-23	1 / 56	Office Open XML Spreadsheet	c33625fe4a0785745525e2cd81f4089512714029d309e65888d66402517fd4fc
2019-02-23	1 / 54	MS Excel Spreadsheet	vbaProject.bin
2019-02-23	1 / 53	MS Excel Spreadsheet	vbaProject.bin
2019-02-23	1 / 56	Office Open XML Spreadsheet	fe117c32e2255a2927fe46cbe012901bf238d308d937596752a0f29f5bb03eaa
2019-02-23	1 / 53	MS Excel Spreadsheet	vbaProject.bin

Rys. 51. Bezpieczeństwo (zrzut ekranu – virustotal.com).

Skan wykonany na virustotal.com wygląda na dość przejrzysty, wszystko wydaje się prawidłowe i nie widać błędów, jednak na kolejnym zrzucie możemy zauważyć kilka nieprawidłowości. Witryna może nie ma dużo błędów lecz istnieje możliwość zaatakowania w celu przechwycenia użytecznych informacji.

Skan za pomocą **pentest-tools.com**:

https://www.lidl.pl/

Summary

Overall risk level: Low

Risk ratings:
High: 0
Medium: 0
Low: 2
Info: 8

Scan information:
Start time: 2021-01-25 00:31:45 UTC+02
Finish time: 2021-01-25 00:32:27 UTC+02
Scan duration: 42 sec
Tests performed: 10/10
Scan status: Finished

Findings

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set

Details

Risk description:
Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:
https://owasp.org/www-community/attacks/Clickjacking

Recommendation:
We recommend you to add the `X-Frame-Options` HTTP response header to every page that you want to be protected against Clickjacking attacks.
More information about this issue:
https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Robots.txt file found

https://www.lidl.pl/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file.

Recommendation:
We recommend you to remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

More information about this issue:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Rys. 51. Bezpieczeństwo (zrzut ekranu – pentest-tools.com).

Google Chrome - Pomoc

Opisz problem

Bezpieczna

Informacje przesyłane i odbierane na tej stronie są prywatne.

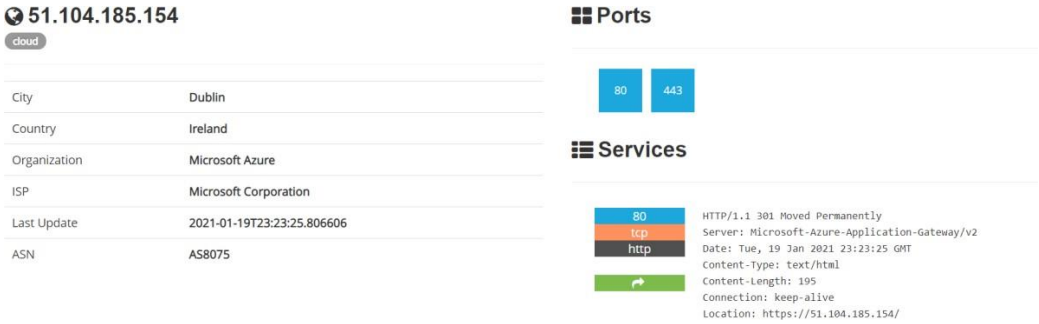
Nawet gdy ta ikona jest widoczna, zawsze zachowuj ostrożność przy udostępnianiu informacji prywatnych. Sprawdź na pasku adresu, czy jesteś na właściwej stronie.

Rys. 52. Bezpieczeństwo (zrzut ekranu – Google Suport).

Na zamieszczonych zrzutach możemy zauważyć nieobecność X-frame-Options, która chroni przed atakami Clickjacking'u, czyli nakładania użytkownikowi do kliknięcia czegoś innego niż to co widzi. Dzięki X-frame-Options (w tym przypadku nie występuje) jesteśmy chronieni przed potencjalnym udostępnieniem naszych informacji poufnych bądź straceniem kontroli nad komputerem. Jest to rozwiązanie warte wprowadzenia na tak często użytkowaną stronę, na której użytkownicy wprowadzają swoje dane do logowania, a także robią zakupy internetowe z zapłatą.
Serwer komunikuje się z przeglądarką za pomocą protokołu http, który nie szyfruje danych. Lepszym rozwiązaniem w tym przypadku byłby HTTPS. Strona uznana jest jako bezpieczna przez Google (Rys.40) jednak warto zachować ostrożność.

10. Stosowane urządzenia sieciowe.

Na tej stornie (lidl.pl) używane są sewery z wykorzystaniem Microsoft Azure. Wszystkie serwery posiadają systemy operacyjne z rodziny Microsoft Windows. Za pomocą witryny shodan.io możemy dowiedzieć się, ze jest ich 9 i każdy pracuje wyżej opisanym systenie operacyjnym. Rozmieszczone są one głównie w Holandii i Irlandii (Rys.42). Możemy
zauważyć, że serwery mają status keep-alive, więc cały czas pracują (Rys 41). Więcej informacji nie udało mi się znaleźć.



Rys. 53. Sprzęt (zrzut ekranu – shodan.io).

Rys. 54. Rozmieszczenie serwerów (zrzut ekranu – shodan.io).

11. Źródła niesklasyfikowane.

W tym podpunkcie został przeanalizowany kod źródłowy strony.

```
...<!DOCTYPE html> == $0
 <!--[if IEMobile 7 ]>
 <html lang="pl-PL" class="no-js iem7"></html><![endif]-->
 <!--[if lt IE 7 ]>
 <html lang="pl-PL" class="no-js ie6"></html><![endif]-->
 <!--[if IE 7 ]>
 <html lang="pl-PL" class="no-js ie7"></html><![endif]-->
 <!--[if IE 8 ]>
 <html lang="pl-PL" class="no-js ie8"></html><![endif]-->
 <!--[if IE 9 ]>
 <html lang="pl-PL" class="no-js ie9"></html><![endif]-->
 <!--[if (gte IE 11)|(gt IEMobile 7)|!(IEMobile)|!(IE)]><!-->
 <html lang="pl-PL" class="js touchevents supports cssfilters flexbox flexboxlegacy">
   <!--<![endif]-->
  ▶<head>…</head>
  ▼<body data-controller="page" class="page" itemscope itemtype="http://schema.org/WebPage" data-ga-environment="dev" data-dynamics-id="CE310A900DE607A5D
 2FC2CC224EE8D8C">
    ▶<noscript>…</noscript>
    ▼<noscript>
       "
                <section class="page__section">
                    <article tabindex="-1" class="hint hint--spaced hint--danger">
                        <header class="hint__header">
                                <span class="hint__icon-container">
                                    <span class="icon icon--danger icon--no-pointer-events icon--small icon--medium@md">
                                        <svg role="img">
                                          <title>Brak Javascriptu</title>
                                          <use xlink:href="/bundles/cakecomponents/dist/images/icon__sprite.svg#danger"></use>
                                        </svg>
                                    </span>
                                </span>
                            <h2 data-controller="hint/title"
                                class="hint__title">Brak Javascriptu</h2>
                        </header>

       "
    </noscript>
  ▼<header data-controller="page/header" class="page__header">
    ▶<div class="page__preheader">…</div>
    ▶<div class="page__masthead">…</div>
    </header>
  ▼<iframe height="0" width="0" style="display: none; visibility: hidden;" src="//9172129.fls.doubleclick.net/activityi;src=9172129;type=pageview;cat…n
 formacje-prawne%2Fpolityka-cookies;~oref=https%3A%2F%2Fwww.lidl.pl%2Fpl?">
    ▶#document
    </iframe>
  ▼<div id="pageMain" tabindex="-1" class="page__main page__main--flex-column" data-controller="page/main" style="margin-top: 50px;">
    ▼<section class="page__section page__section--hero">
      ▶<div class="hero" data-controller="hero/main/_6b5olqumb">…</div>
        ::after
      </section>
    ▼<section class="page__section page__section--tab-nav">
      ▶<div class="tabnavaccordion__wrapper" data-container="tabnavaccordion__wrapper" data-controller="tabnavaccordion/width">…</div>
        ::after
      </section>
    ▶<section class="landing-page__zone--254410" data-ez-zone-id="254410">…</section>
      ::after
    </div>
  ▼<script type="text/javascript" id>
      window.gaOptin=function(){setTimeout(function(){for(var b=dataLayer.length,a=0;a<b;a++)dataLayer.push(dataLayer[a])},100)};
    </script>
  ▼<script type="text/javascript" id>
      var disableStr="ga-disable-"+google_tag_manager["GTM-N39L9N"].macro(26);
      function gaOptout(){document.cookie=disableStr+"\x3dtrue; expires\x3dThu, 31 Dec 2099 23:59:59 UTC;
      path\x3d/";window[disableStr]=!0;document.cookie="_ga\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC;
      domain\x3dlidl.pl;path\x3d/";document.cookie="_gat_UA-66134079-23\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC; domain\x3dlidl.pl;
      path\x3d/";document.cookie="_dc_gtm_UA-66134079-23\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC; domain\x3dlidl.pl; path\x3d/";alert("Ciasteczko
      zosta\u0142o ustawione")}
      ;
```

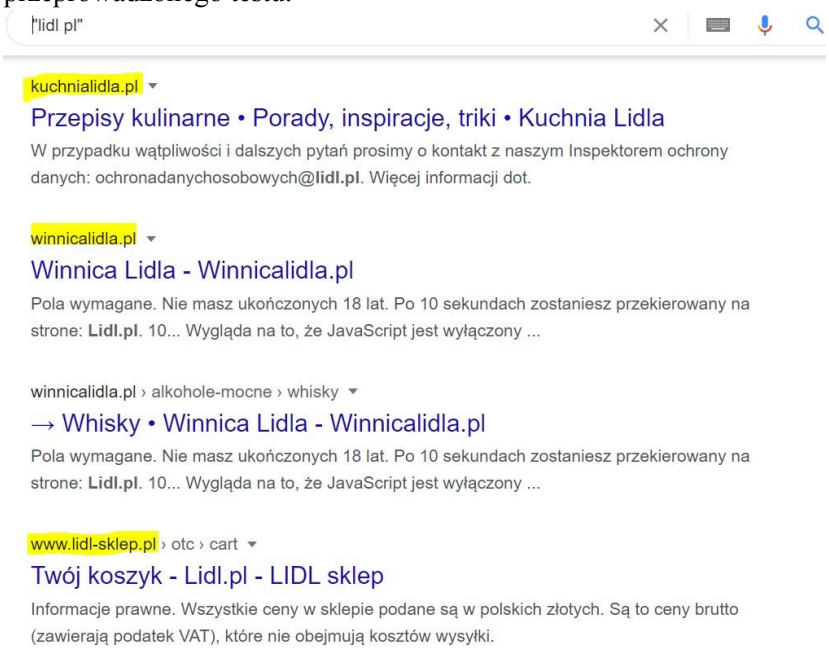
```
  </script>
▼<script type="text/javascript" id>
   var disableStr="ga-disable-"+google_tag_manager["GTM-N39L9N"].macro(26);
   function gaOptout(){document.cookie=disableStr+"\x3dtrue; expires\x3dThu, 31 Dec 2099 23:59:59 UTC;
   path\x3d/";window[disableStr]=!0;document.cookie="_ga\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC;
   domain\x3dlidl.pl;path\x3d/";document.cookie="_gat_UA-66134079-23\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC; domain\x3dlidl.pl;
   path\x3d/";document.cookie="_dc_gtm_UA-66134079-23\x3d; expires\x3dThu, 01 Jan 1970 00:00:00 UTC; domain\x3dlidl.pl; path\x3d/";alert("Ciasteczko
   zosta\u0142o ustawione")}
   ;
  </script>
▶<footer class="page__footer">…</footer>
▶<script type="text/javascript" data-cookieconsent="marketing">…</script>
  <script type="text/javascript" data-cookieconsent="marketing" src="https://lidl.media01.eu/tm_js.aspx?trackid=3244CEA8CF8D1F9240AB120A76DB9EA0&mode=
  2&dt_freetext=&dt_subid1=&dt_subid2=&dt_keywords=" async="async"></script>
  <script defer src="/bundles/cakecomponents/vendor/requirejs/require.js"></script>
▶<script>…</script>
▼<script>
            document.addEventListener('DOMContentLoaded', function () {
                require(['FrontPage']);
            });

  </script>
▼<iframe height="0" width="0" style="display: none; visibility: hidden;" src="//9172129.fls.doubleclick.net/activityi;src=9172129;type=pageview;cat…=
Polish%20z%C5%82oty;u32=undefined;~oref=https%3A%2F%2Fwww.lidl.pl%2Fpl?">
  ▶#document
  </iframe>
  <script type="text/javascript" async src="https://lidl.media01.eu/tm.js?v=8F14E45FCEEA167A5A36DEDD4BEA2543"></script>
  <script>var dynamic_tm_data_new = { "lidl_ga_cookie": "false"};</script>
▼<script type="text/javascript" id>
   (function(){window.addEventListener("beforeunload",function(){window.dataLayer.push({event:"scrollDepth"})})})();
  </script>
</body>
</html>
```

Rys. 55. Analiza kodu (zrzut ekranu – lidl.pl).

Dzięki analizie wyżej podanego kodu możemy zobaczyć wiele odnośników do stron co czyni kod tak długim (niektóre funkcje zwinąłem). Nie było możliwe wklejenie całego kodu źródłowego, ponieważ zajmował około 50 stron. Analiza pozwoliła stwierdzić w jakim języku jest napisana strona. Nie przyniosło to za dużo informacji.

12. Inne.

Poprzez wyszukiwanie zaawansowane frazy „lidl.pl”, wyświetlają nam się w przeglądarce poddomeny związane z główną stroną witryny. Nie wnosi to dużo do przeprowadzonego testu.



Rys. 56. Inne (zrzut ekranu – google.com).

13. Wnioski ogólne.

Na projekt mieliśmy dużo czasu. Przez ten czas można było bardzo dokładnie go wykonać czy użyciu różnych narzędzi, a nie opierać się tylko na jednych. Eksperyment pokazał, że metody, a także strony internetowe umożliwiające wykonywanie tych czynności są dość leciwe lecz skuteczne. Wykonany test nie uwzględnia wszystkich metod i narzędzi możliwych do wykorzystania w celu uzyskania rekonesansu pasywnego testów penetracyjnych. Dzięki tym narzędziom uzyskane zostały informacje, które mogłyby interesować potencjalnego intruza.

Lidl jest dużą firmą, niemożliwe było uzyskanie typowo osobowych danych odnośnie pracowników zarządu. Na żadnym sprawdzanym profilu członków zarządu nie było
podpiętego e-maila pod profilem na LinkedIn.com (na innych portalach społecznościowych nie udało mi się ich odnaleźć). Mogliśmy tylko uzyskać informacje odnośnie ich
wykształcenia, zainteresowania, a także pełnionej roli w firmie Lidl i poprzednich stanowiskach.

Podczas przeprowadzania testu, strona posiadła status bezpiecznej stwierdzony przez Google, jednak możliwy był atak ClickJacking'u. Doświadczona osoba może to sprawnie wykorzystać w celu uzyskania prywatnych informacji użytkownika (np. adres zamieszkania, wynikający z realizowanych przesyłek, a także informacje o płatnościach internetowych). Strona jest bardzo rozbudowana co pokazuje również, że posiada niedopracowania. Na przestrzeni lat i tak diametralnie się zmieniła i wyprzedza strony innych sieci sklepów spożywczych.

Podsumowując uważam, że projekt wszystkie punkty i założenia projektu zostały spełnione i wykonane. Dzięki temu zadaniu zyskałem dużo informacji na temat narzędzi wykorzystywanych w takich sytuacjach i zyskana tu wiedza na pewno mi się jeszcze przyda. Trzeba uważać na wprowadzane treści i być ostrożnym, bo nawet strony internetowe tak dużych firm jak Lidl posiadają niedociągnięcia i niedoskonałości.