



WYDANIE SPECJALNE NR 1

dot.pl



NASK



dot.pl

RAPORT PODSUMOWUJĄCY 2023

WYDANIE SPECJALNE NR 1

WARSZAWA, MAJ 2024



ISBN: 978-83-65448-86-6

aid.pl mail.pl com.pl
agro.pl atm.pl edu.pl
gmina.pl info.pl mil.pl
targi.pl mil.pl gsm.pl
miasta.pl media.pl
realestate.pl shop.pl
net.pl kolobrzeg.pl
nieruchomosci.pl
szkola.pl org.pl
sklep.pl sos.pl
travel.pl gniezno.pl
nom.pl turystyka.pl

Spis treści

- 4 Wstęp

- 7 **CZĘŚĆ I**
Rynek nazw domen .pl

- 8 Fakty i liczby
- 9 Ranking europejskich rejestrów domen
- 10 Obsługa domen
- 17 Obsługa abonentów nazw domen .pl
- 19 Wypowiedzi Partnerów Rejestru domen .pl
- 24 Podział rynku nazw domen .pl

- 27 **CZĘŚĆ II**
Internet oczami ekspertów z branży DNS

- 31 Popularność e-usług
- 37 Zagrożenia w sieci
- 41 Nienawiść w Internecie
- 47 Bezpieczeństwo cyfrowe klientów
- 53 Rynek i promocja on-line

Wstęp

Technologie informacyjne i komunikacyjne stwarzają nowe możliwości powszechnej konsumpcji. Dotyczy to także konsumpcji informacji. Dzisiaj paradygmat konsumenta zostaje zastąpiony paradygmatem użytkownika sieci – klienta, osoby której dane cyfrowe, treści cyfrowe, także generowane w ramach *Internet behaviour*, są powszechnie monetyzowane i wykorzystywane do działań marketingowych, w ramach profilowania i targetowania. Coraz częściej działania te obejmują szeroko rozumiane aktywności związane ze świadczeniem zróżnicowanych usług cyfrowych. Jednak trzeba pamiętać, iż sam Internet przestaje być jednolitą całością. Jako obszar rozszczerpiony jest miejscem walki o władzę nad rozwijającymi się nowymi technologiami. Poza towarem, tak cennym jak dane, pojawia się wojna o przestrzeń wolności słowa, o prywatność, o prawo własności cyfrowej, o wolność gospodarczą.

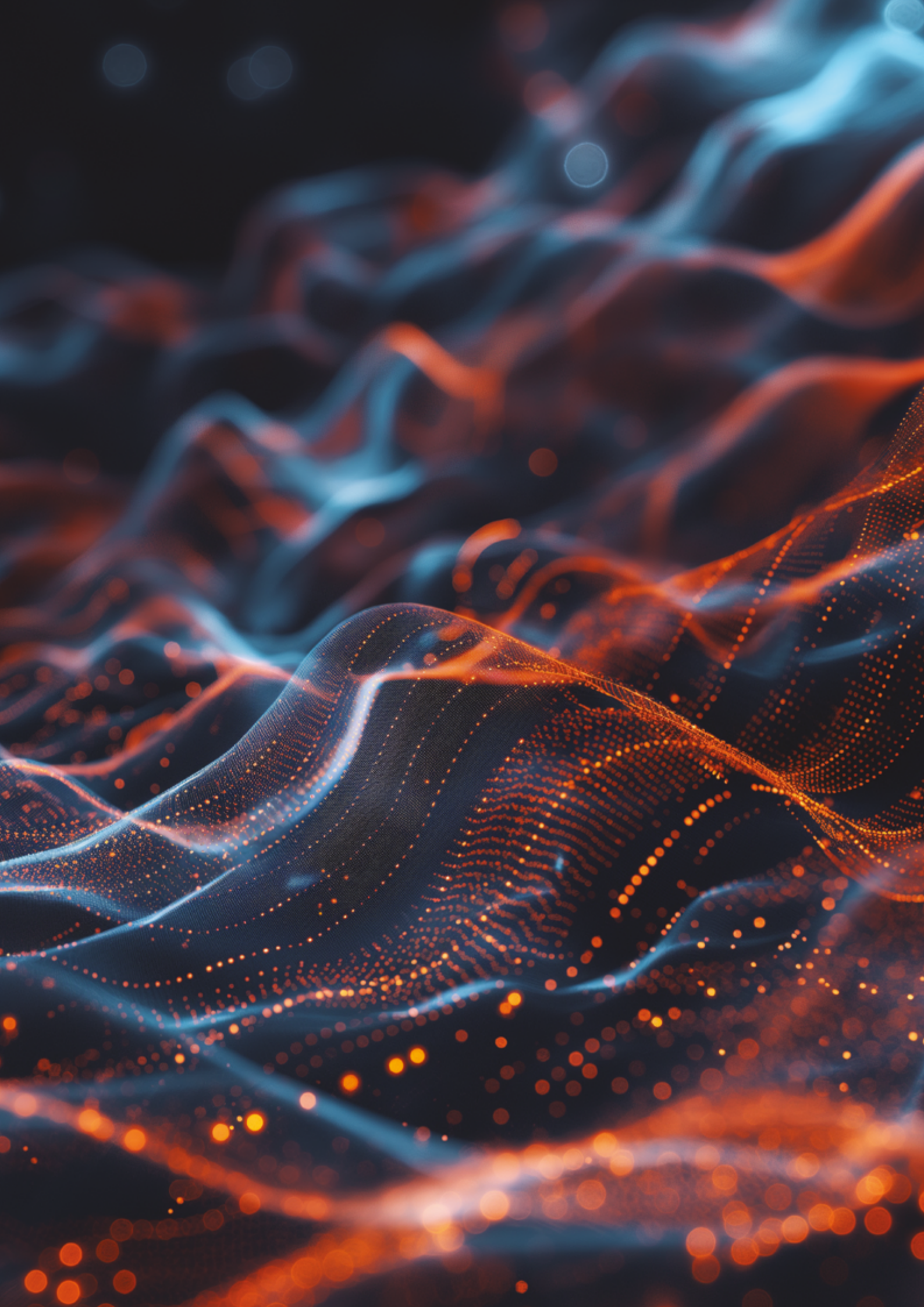
Paul Baran, naukowiec polskiego pochodzenia, to przykład osoby, która zdecydowanie wyprzedziła swój czas. Dziś wiemy, że choć jego wizje przyszłości nie znalazły uznania w latach 60., to *de facto* sprawdziły się. Dzięki współpracy z Rand Corporation, organizacją badawczą działającą przy amerykańskich powietrznych siłach zbrojnych, Paul Baran rozwinął swój projekt, opisując go w 11-tomowej monografii pt. „On Distributed Communications”, opublikowanej w 1964 r. Był także autorem artykułu naukowego opublikowanego w Rand Paper (P-3717) pt. „Some changes in information technology affecting marketing in the year 2000” (lipiec 1968 r.). Paul Baran opisał w nim wizję przyszłości – roku 2000, wskazując rozwój e-commerce, opartego w znacznej mierze na komunikacji drogą elektroniczną oraz idei sklepów wirtualnych. Dzisiaj wizja ta nie jest krytykowaną iluzją a faktem i naszą codziennością. Podstawową konsekwencją zmian technologicznych stało się pojawienie nowej przestrzeni funkcjonowania jednostki, grup społecznych czy nawet państwa. Jest nią cyberprzestrzeń. Dzisiaj jej analiza i próba zdefiniowania to praktycznie konieczność ustalenia zakresu przestrzennego oddziaływania norm prawnych odnoszących się do nowych technologii. Przestrzeń ta związana jest z systemem domen internetowych, jak również z innymi środowiskami funkcjonowania wszystkich nas w sieci, także w mediach społecznościowych. 20 kwietnia 1992 r. zarejestrowano pierwszą krajową domenę najwyższego stopnia z końcówką .pl. W pierwszych latach XXI wieku ich liczba sięgała 200 tys., aby w 2024 r. osiągnąć poziom 2,5 mln.

Z nowymi mediami związane są działania korporacji – przedsiębiorców, których głównym celem jest zysk, wygenerowany m.in. poprzez handel w sieci, oraz towarzyszące mu działania reklamowe. Dlatego analiza tych technik pozwoli na dokładne ustalenie przyszłych problemów związanych z funkcjonowaniem cyberprzestrzeni i związanego z nią środowiska sieciowego. Identyfikacja zagrożeń związanych z usługami sieciowymi oraz przegląd aktualnych zagadnień związanych z ochroną własności w sieci pozwolą postawić diagnozę, co do konieczności redefinicji celów przyszłej regulacji w obszarze uprawnień właścicielskich związanych monopolem, uprawnionych do dóbr niematerialnych, takich jak prawo autorskie i prawa pokrewne, tajemnica przedsiębiorcy, know-how, przedmioty ochrony własności przemysłowej oraz bazy danych. Zgodnie z ideą Petera Weibela, obok cyfrowego myślenia, którego oddziaływanie i sukcesy objęły już cały świat (bez „maszyn liczących” nie funkcjonowałyby bowiem żadne lotniska, fabryki, dworce, centra zakupowe, szpitale i inne) pojawia się również cyfrowa sztuka, która zyskuje na znaczeniu i popularności. Warto dodać, że kluczowym aspektem tego rozwoju staje się bezpieczeństwo. Kolejnym ważnym elementem rozwoju tego rynku jest potrzeba bezpieczeństwa, która wynika z kreacji wyzwalanej przez innowacje i nowe technologie. Taką własnością w sensie faktycznym jest domena internetowa a kluczową jej cechą jest jej bezpieczny wymiar.

Dzisiaj aktywność w Internecie podlega uprzedniej rejestracji domeny internetowej, która pozwala uprawnionemu na prowadzenie strony internetowej w warunkach rynkowych, z jednoczesnym zastrzeżeniem tych działań w oparciu o porządek i bezpieczeństwo publiczne. Domena internetowa w hydrancie informacji i chaosie BIG DATA, daje pewność identyfikacji własnego środowiska cyfrowego. Eksterytorialność sieci przyczyniła się do stworzenia globalnego systemu rejestracji domen internetowych. Przyjęte zasady stworzyły możliwości nadawania najróżniejszych nazw domenom w warunkach „kto pierwszy, ten lepszy”, co nadaje konkretnemu środowisku cyfrowemu spersonalizowany profil.

Przygotowany przez Rejestr domeny .pl w NASK-PIB raport dotyczący rozwoju rynku domen, ale także próba przeglądu i redefinicja trendów w świecie cyfrowym, pozwoli w przyszłości dokonać oceny przyjętych standardów ochrony tego środowiska. Wnioski z tej analizy mogą stanowić wstęp do poszerzonej diagnozy związanej z nowym etapem rozwoju ery cyfrowej.

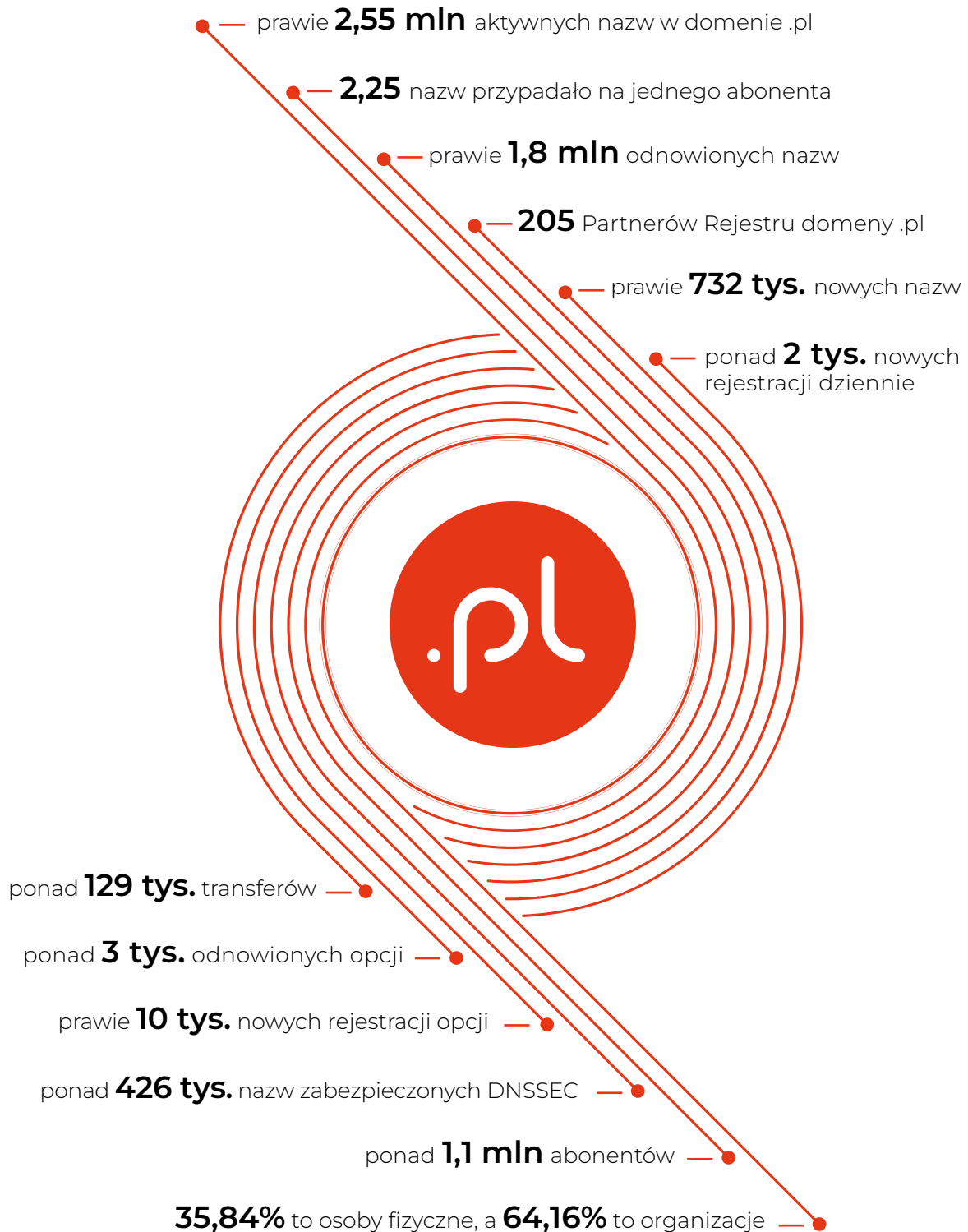
Zapraszamy do lektury!



CZĘŚĆ I

**Rynek nazw
domeny .pl**

Fakty i liczby



Ranking europejskich rejestrów domen



Niemcy **.de** **17 653 764**



Wielka Brytania **.uk** **10 732 479**



Holandia **.nl** **6 288 394**



Francja **.fr** **4 133 832**



Włochy **.it** **3 497 624**



Polska **.pl** **2 546 407**



Hiszpania **.es** **2 095 642**



Belgia **.be** **1 734 182**



Szwecja **.se** **1 478 955**

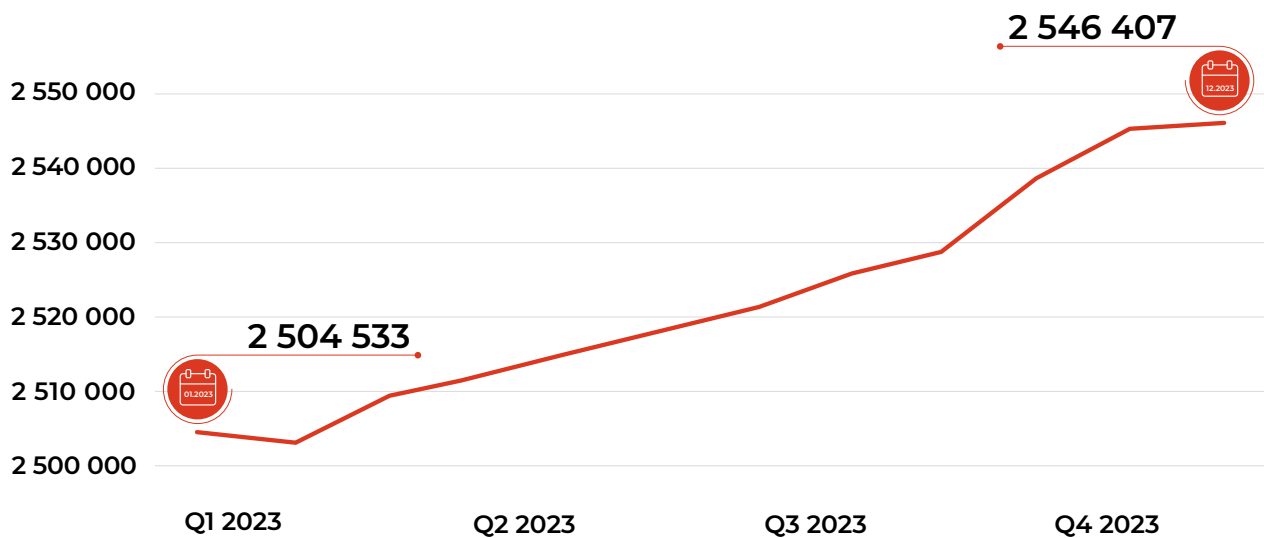


Czechy **.cz** **1 468 788**

Obsługa domen

Liczba nazw utrzymywanych w domenie .pl

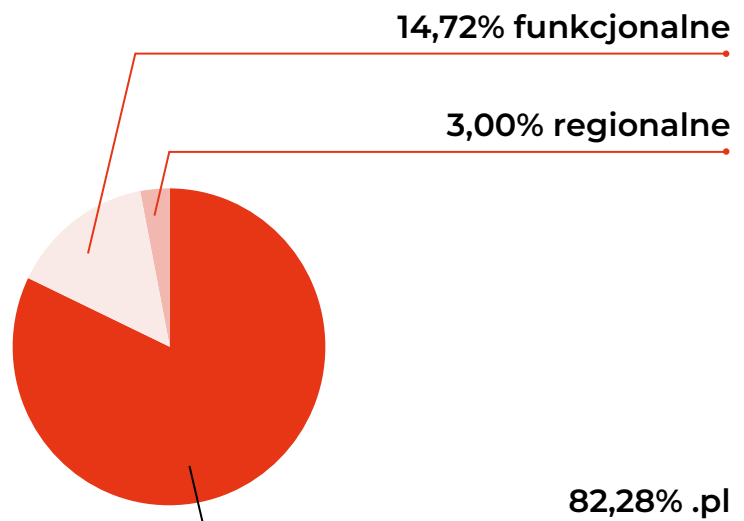
W 2023 roku o **36 151** zwiększyła się liczba aktywnych w DNS nazw domeny .pl, a dynamika roczna wyniosła **1,44%**.



Copyright by NASK

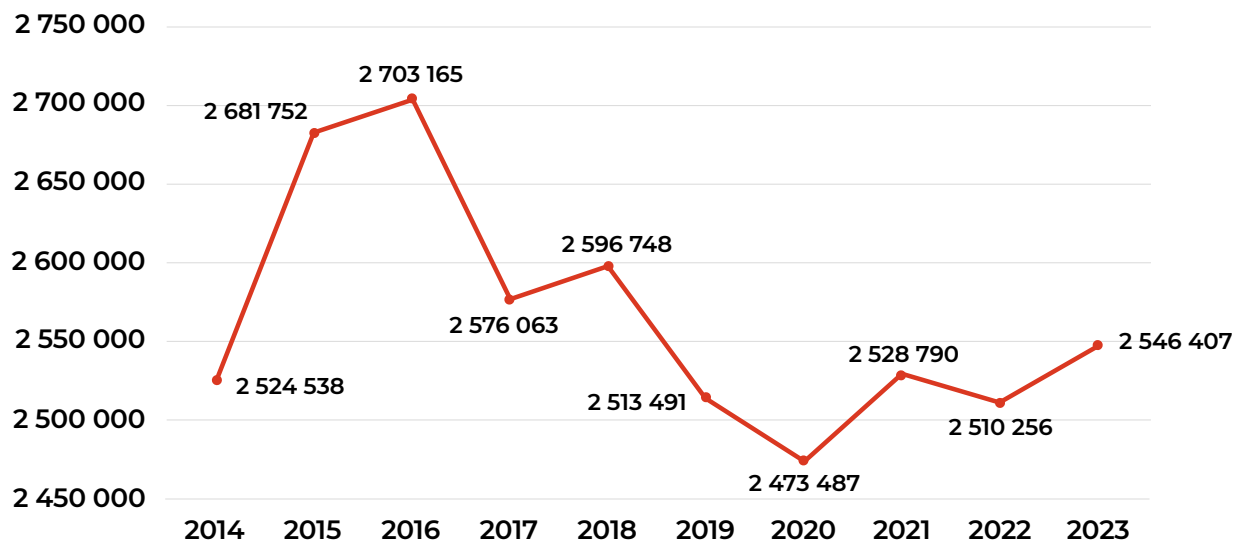
Aktywne w DNS nazwy domeny .pl z podziałem na typ strefy

Podział nazw na znajdujące się bezpośrednio w domenie .pl, w domenach funkcjonalnych, tj. com.pl, edu.pl i innych, oraz w domenach regionalnych, np. waw.pl, bieszczady.pl i innych.



Copyright by NASK

Liczba nazw domeny .pl w DNS, lata 2014–2023



Copyright by NASK

Liczba rejestracji nazw domeny .pl

2023 rok



liczba rejestracji
731 748



średnia dzienna liczba
rejestracji nazw
2 005



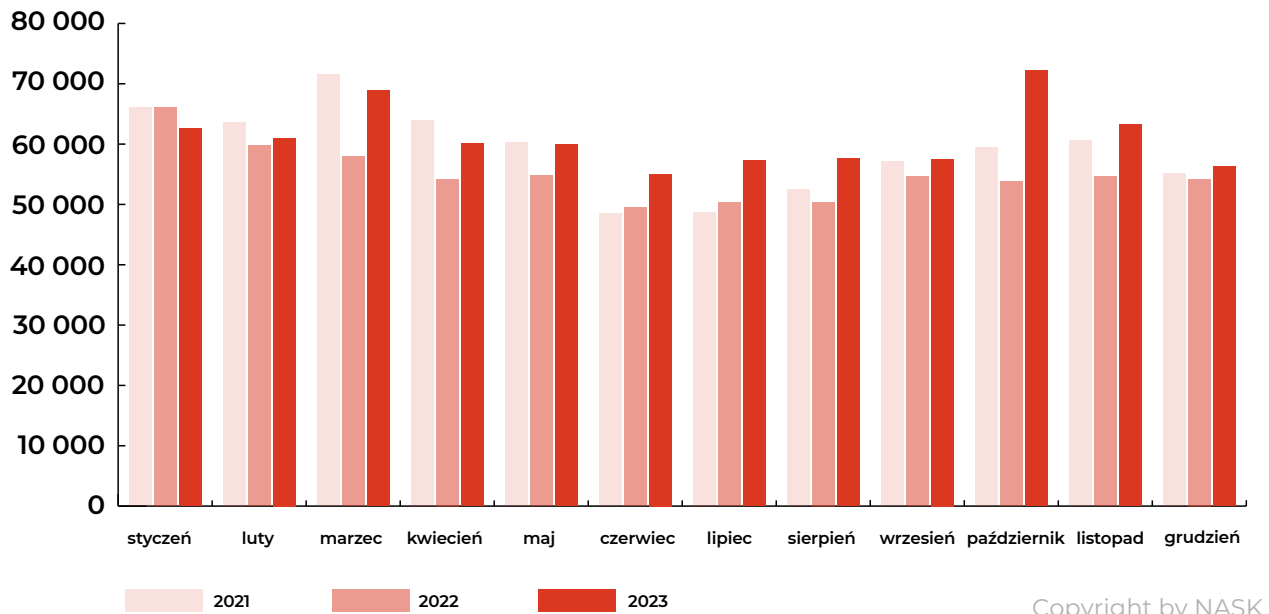
najwięcej domen
zarejestrowano
w październiku
72 237



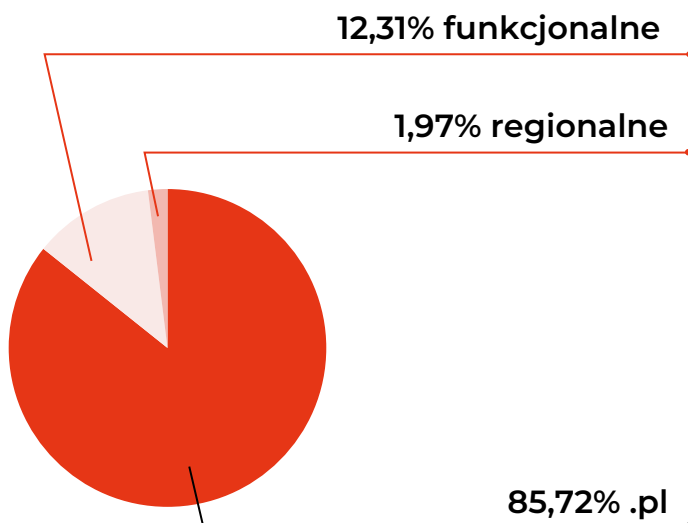
najmniej domen
zarejestrowano
w czerwcu
55 052

Copyright by NASK

Liczba rejestracji nazw domeny .pl



Rejestracje nazw domeny .pl podzielone na typ strefy



Podział nazw na znajdujące się bezpośrednio w domenie .pl, w domenach funkcjonalnych, tj. com.pl, edu.pl i innych, oraz w domenach regionalnych, np. waw.pl, bieszczady.pl i innych.

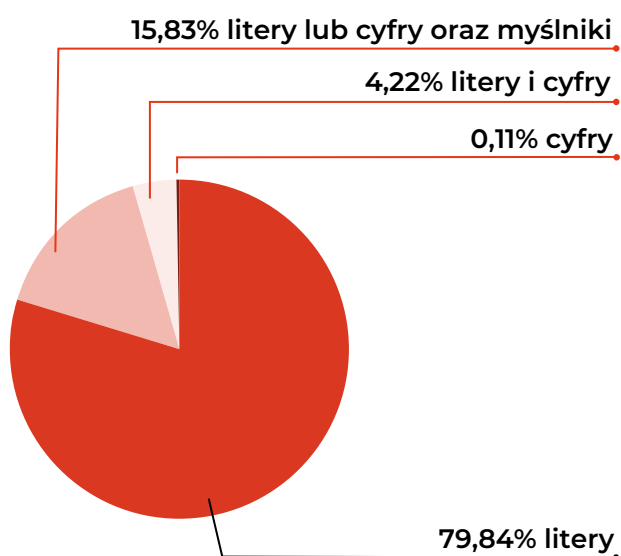
Struktura nazw domeny .pl

Średnia liczba znaków używanych w nazwach domeny .pl na koniec 2023 roku wyniosła **10,93**.

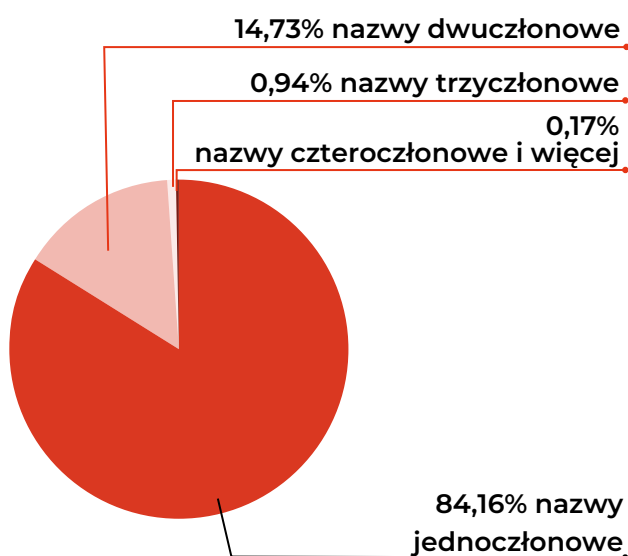
Maksymalną liczbę **63** znaków miało **8** nazw domeny .pl.

Najbardziej powszechne były nazwy **dziewięcioznakowe**, w rejestrze było ich **229 390**.

Maksymalna liczba członów występujących w jednej nazwie, odnotowana na koniec 2023 roku, wyniosła **26**.

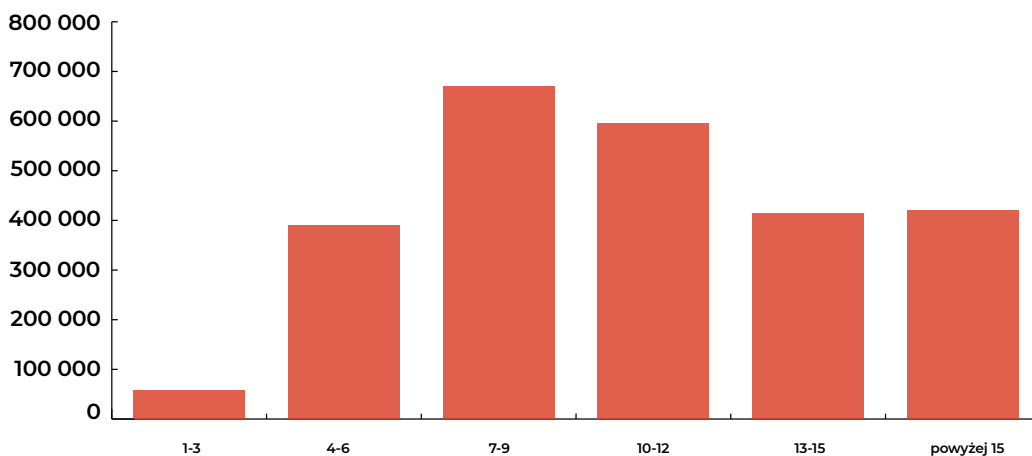


Znaki w nazwach domeny .pl, 2023



Liczba członów w nazwach domeny .pl, 2023

Copyright by NASK

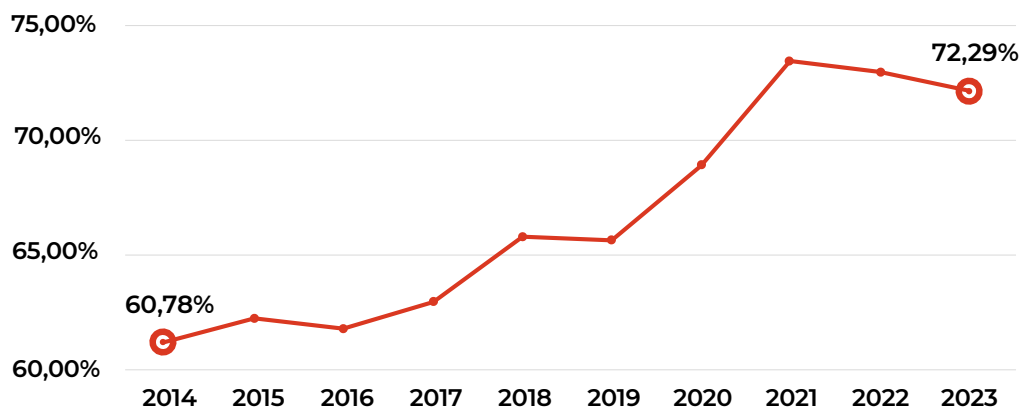


Liczba znaków w nazwach domeny .pl, 2023

Copyright by NASK

Odnowienia nazw domeny .pl
na kolejny okres rozliczeniowy

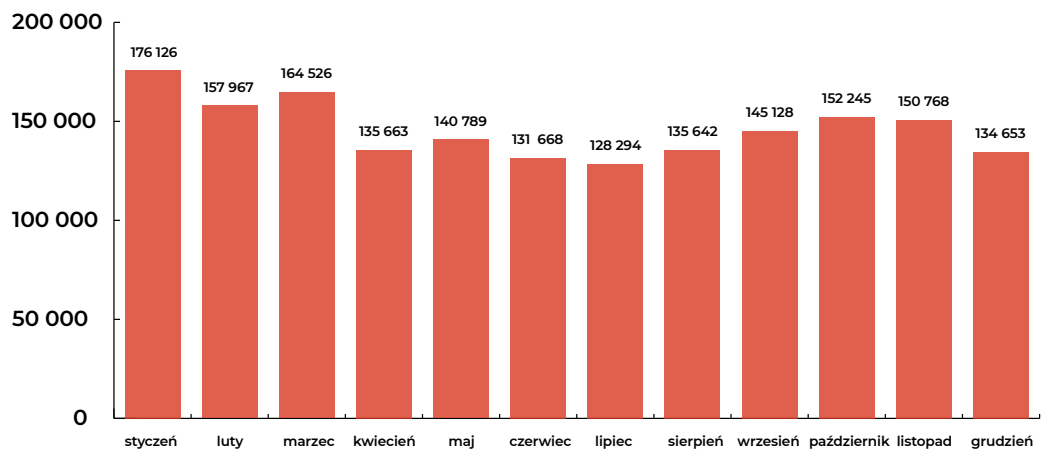
lata 2014–2023



Procent odnowień nazw domeny .pl, lata 2014–2023

Copyright by NASK

2023 rok

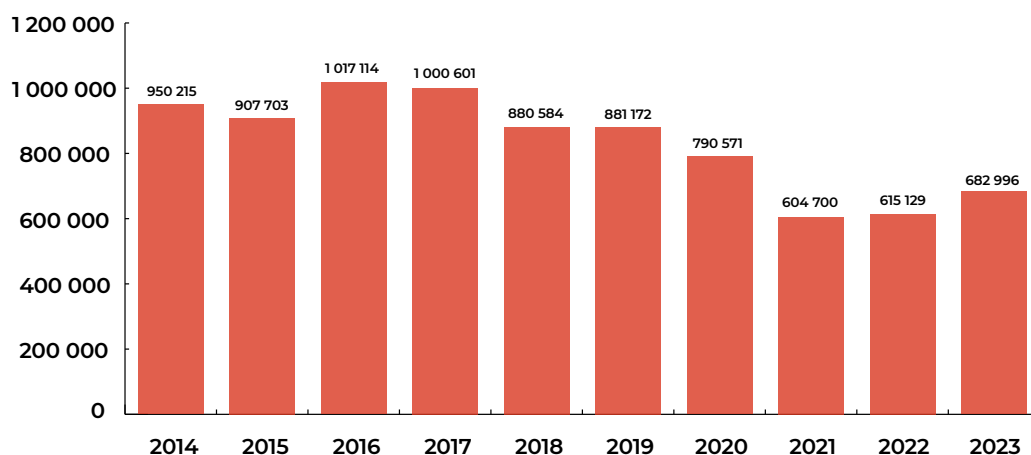


Liczba odnowionych nazw domeny .pl, 2023

Copyright by NASK

Liczba nieodnowionych nazw domeny .pl

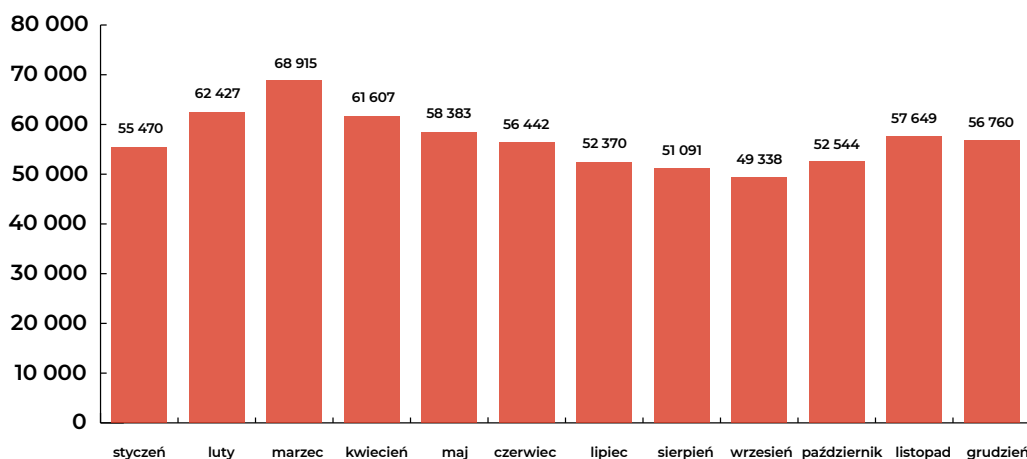
lata 2014–2023



Liczba nazw domeny .pl uwolnionych z powodu braku odnowienia, lata 2014–2023

Copyright by NASK

2023 rok

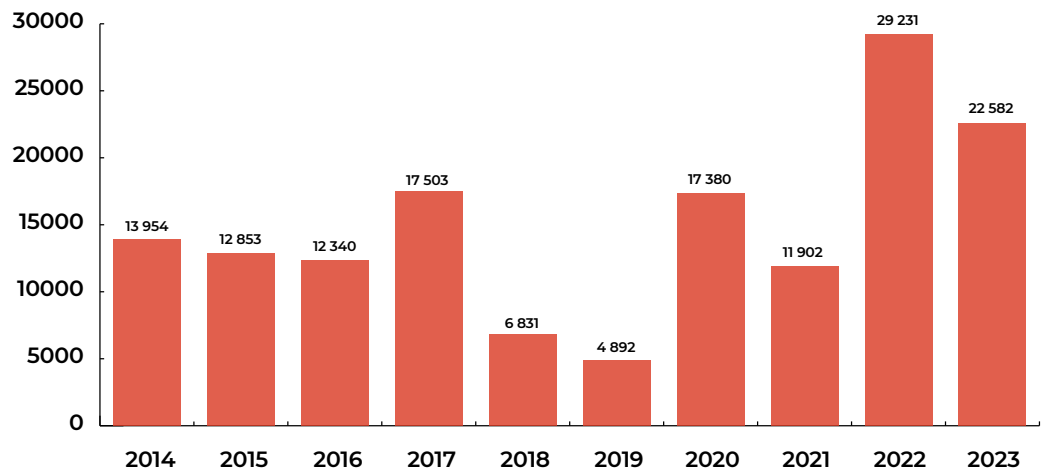


Liczba nazw domeny .pl uwolnionych z powodu braku odnowienia, 2023

Copyright by NASK

Liczba usuniętych nazw domeny .pl

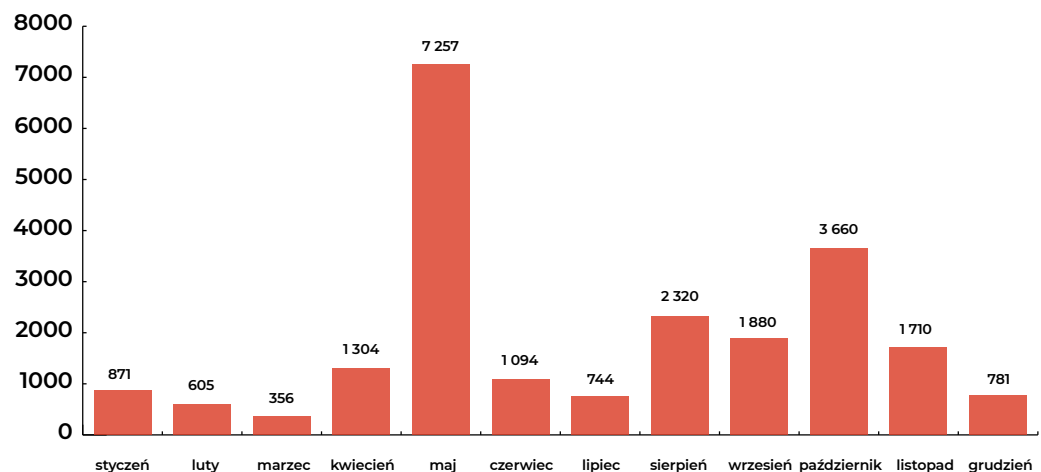
lata 2014–2023



Liczba nazw domeny .pl uwolnionych po wcześniejszym usunięciu, lata 2014–2023

Copyright by NASK

2023 rok

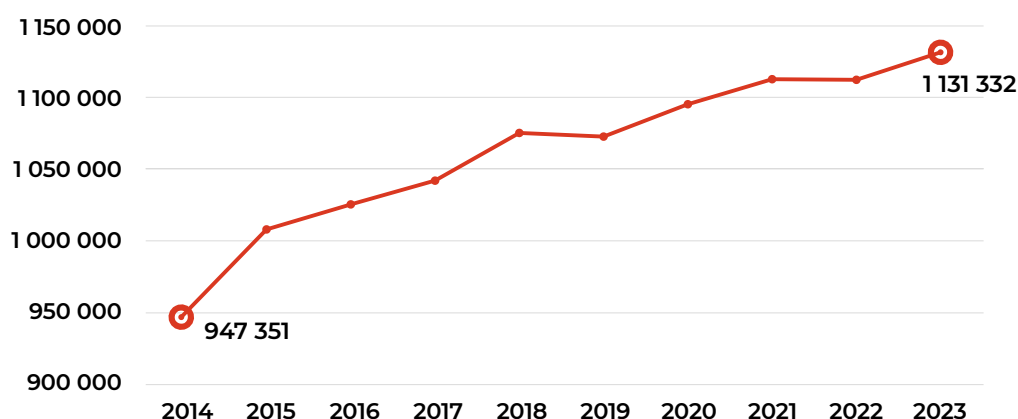


Liczba nazw domeny .pl uwolnionych po wcześniejszym usunięciu, 2023

Copyright by NASK

Obsługa abonentów nazw domeny .pl

Liczba abonentów nazw domeny .pl



Liczba Abonentów, lata 2014–2023

Copyright by NASK

18 983 liczba abonentów, którzy dołączyli w 2023 roku

170 322 liczba zmian abonenta nazw domeny .pl w 2023

2,25 nazw domeny .pl średnio na jednego abonenta

64,16% abonentów to organizacje

35,48% abonentów to osoby fizyczne

Copyright by NASK

Lokalizacja abonentów domeny .pl

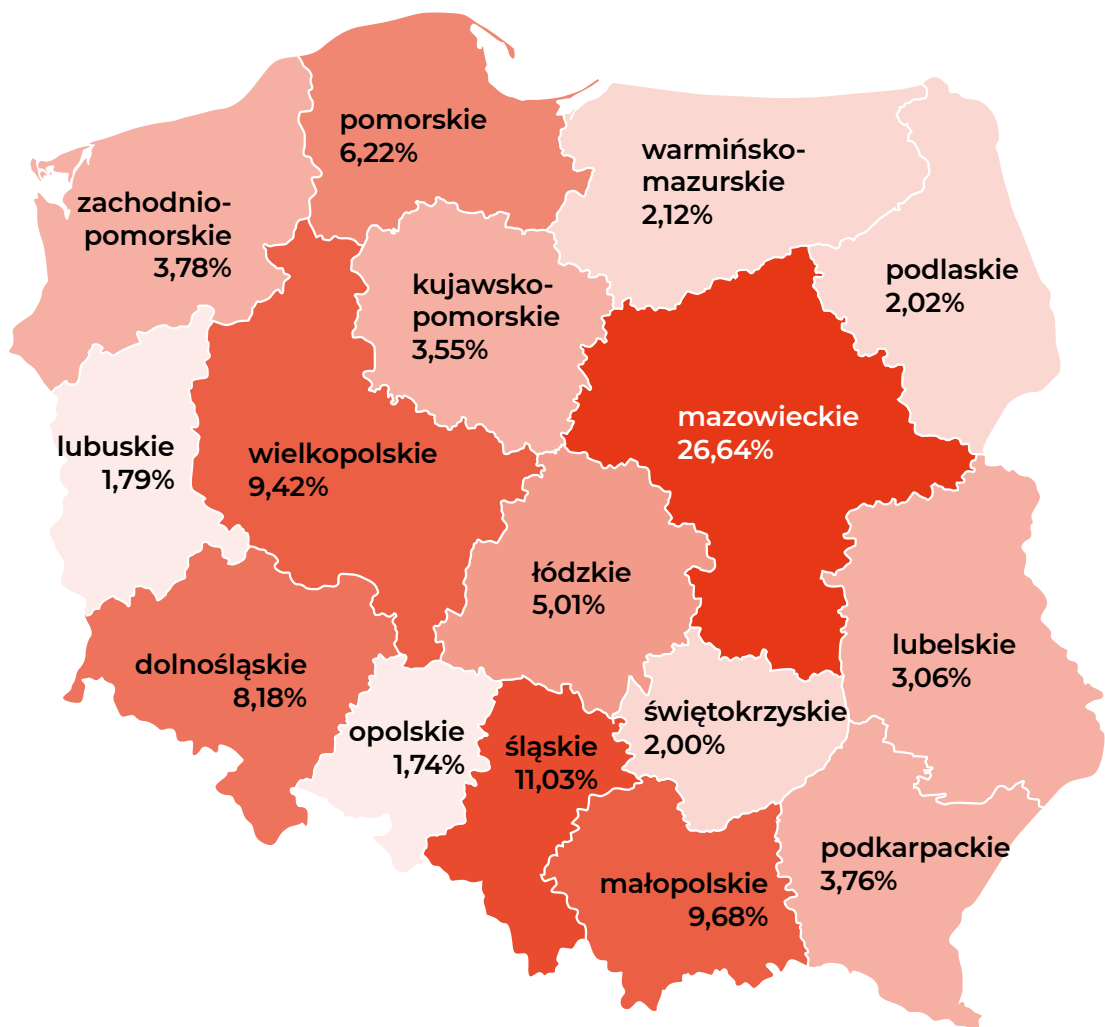
90,56% nazw domeny .pl istniejących w DNS na koniec 2023 roku, utrzymywanych na rzecz abonentów z Polski

26,64% nazw było zarejestrowanych na rzecz osób i organizacji z województwa mazowieckiego, z czego aż 18,87% z Warszawy

Prawie połowę wszystkich abonentów z Polski stanowili użytkownicy domen z województw:

26,64% mazowieckiego
11,03% śląskiego
9,68% małopolskiego

Copyright by NASK



Lokalizacja abonentów w Polsce, z podziałem na województwa, 2023

Copyright by NASK

Wypowiedzi Partnerów Rejestru domeny .pl

Home.pl S.A.

home.pl

Rok 2023, podobnie jak lata ubiegłe, jasno pokazał, że .pl jest ulubioną domeną polskich abonentów. Statystyki są jednoznaczne: zarówno domeny gTLD, nTLD jak i inne domeny ccTLD są wybierane zdecydowanie rzadziej. .pl jest najchętniej używaną domeną przez Polaków, co wydaje się dość naturalnym utożsamianiem się ze swoją ojczyzną. Pokazuje również, że większość biznesów, albo pomysłów na biznes ma wciąż charakter lokalny i ogranicza się do Polski. Domena .pl ma ugruntowaną i prestiżową pozycję i budzi zaufanie, ale jest dostępna także na przejrzystych warunkach rejestracji. Za jej popularnością przemawia również fakt istnienia Sądu Polubownego ds. Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji (PIIT), który zapewnia abonentom poczucie bezpieczeństwa.

Na przestrzeni całego roku 2023 odnotowaliśmy zwiększone zainteresowanie klientów rejestracją domen .pl względem roku 2022. Dotyczy to głównie rejestracji na drugim poziomie, których przybyło najwięcej. Procentowy udział domen funkcjonalnych i regionalnych w nowych rejestracjach utrzymywał się mniej więcej na podobnym poziomie przez cały rok.

Widzimy, że większość klientów od razu wykorzystuje zakupione domeny do prowadzenia serwisów www i sklepów internetowych. Coraz rzadziej abonenci rejestrują większe liczby domen w celach spekulacyjnych – do dalszej odsprzedaży. Również w związku z tym w roku 2023 obserwowaliśmy wzrost roli domen .pl jako głównego adresu internetowego polskich przedsiębiorców i abonentów indywidualnych. Możliwe, że ze względu na wysoką inflację i optymalizację kosztów klienci częściej je zastępowali mniej popularne rozszerzenia domenami .pl.

Rynek odnowień domen .pl w roku 2023 to rynek ustabilizowany. Notujemy wysoki wskaźnik odnowień domen rejestrowanych w poprzednich latach. Świadczy to o dużej dojrzałości rynku, czemu nie możemy się zresztą dziwić – domena .pl w 2023 obchodziła 33 rocznicę ustanowienia.

Po bardzo udanym dla domeny .pl 2023 roku z optymizmem patrzymy na trwający już 2024.

Consulting Service Sp. z o.o.



Miniony rok przyniósł pewne ożywienie na rynku domeny krajowej. Znajduje to odzwierciedlenie w rosnącej liczbie nowozarejestrowanych nazw domeny .pl a także rosnącym wskaźniku odnowień, co przełożyło się sumarycznie na nieznaczny wzrost aktywnych nazw w domenie .pl w porównaniu do lat 2022, 2021 i 2020.

Zastanawiające jest, czy będzie to początek nowego dobrego trendu dla tego segmentu domen. Nie można przy tym zapominać o domenie .com, która w naszym kraju nadal zdobywa nowych abonentów a jej rynek z numerem jeden pod względem utrzymywanych na świecie nazw domen na razie pozostaje poza zasięgiem innych rozszerzeń. Pomimo wyczerpania się popularnych nazw, a także sukcesywne coroczne podwyżki cen bazowych domena .com jest nadal atrakcyjna zwłaszcza dla podmiotów gospodarczych.

W 2024 roku spodziewamy się kontynuacji wzrostowego trendu na rynku domeny .pl w segmencie nowych rejestracji. Nie bez znaczenia pozostają tutaj wydarzenia za naszą wschodnią granicą i coraz większe zainteresowanie polskimi adresami przez ukraińskie podmioty gospodarcze, które przenosząc swój biznes do Polski przy okazji inwestują w nasze krajowe adresy internetowe.

Jednocześnie zastanawiające jest, czy ze względu na wprowadzone Rozporządzenie DSA a także oczekiwane wdrożenie NIS 2 liczba aktywnych nazw w domenie .pl w roku bieżącym utrzyma się przynajmniej na poziomie z końca 2023 r., biorąc pod uwagę chociażby wymóg aktualizacji niepełnych czy też nierzetelnych danych Abonentów utrzymujących w systemie registry .pl swoje domeny.

nazwa.pl sp. z o.o.



Rok 2023 można nazwać rokiem zmian w procesie rejestracji domen internetowych. Istotnym mechanizmem, który zaczął odgrywać rolę przy podejmowaniu decyzji o wyborze danego adresu, stała się Sztuczna Inteligencja. Obserwując trendy w tym zakresie, nazwa.pl uruchomiła wyszukiwarkę nazw internetowych opartą o technologię AI. Umożliwia ona znalezienie domeny w oparciu o zapytanie w języku naturalnym. Algorytmy Sztucznej Inteligencji nie tylko określają na tej podstawie branżę, lecz także dodatkowo badają słowa kluczowe, które są dla tej branży charakterystyczne. Przekłada się to na propozycje idealnie dopasowanych domen. Szacujemy, że znaczenie technologii AI przy rejestracji adresów będzie rosnąć i zwiększało swój udział dla nowo rejestrowanych nazw.

Rynek polskich domen utrzymuje się na stabilnym poziomie przy rosnącej liczbie aktywnych stron internetowych. Zarejestrowane adresy, które do tej pory utrzymywane były w celach inwestycyjnych, są coraz częściej wykorzystywane do publikacji serwisów, identyfikacji marek, towarów i usług.

Sprzyja to normalizacji rynku, co ma odzwierciedlenie we wskaźnikach odnowień domen.

Z badań nazwa.pl wynika, że ponad 80% zapytań o polskojęzyczne strony WWW pochodzi z obszaru naszego kraju. Domeny, wskazujące na lokalizację podmiotu na terenie Polski, pomagają budować jego prestiż i zwiększają dotarcie do klientów. Choć w nazwa.pl umożliwiamy rejestrację coraz bardziej popularnych domen nTLD, które nawiązują do branży lub charakteru prowadzonego biznesu, to trzeba przyznać, że polskie rozszerzenia cieszą się niestąbną popularnością.

Rynek domen to dziś rynek konkurencyjny. Spośród licznych ofert klient może wybrać takie, które najlepiej odpowiadają jego oczekiwaniom. Podstawowe rozwiązania na ogół charakteryzują się cenami zbliżonymi do cen hurtowych NASK. Dostępne są również rozwiązania premium, takie jak pakiet „Bezpieczna domena” w nazwa.pl. W tym przypadku użytkownik otrzymuje wraz z nazwą internetową, szereg ważnych funkcjonalności i usług. Mowa w szczególności o zabezpieczeniach, tak ważnych w cyfrowym świecie. Wymienić wśród nich można obsługę domen na geograficznie rozproszonych serwerach DNS Anycast, która zapewnia jej wyższy poziom ochrony i niezawodność działania. Pakiet „Bezpieczna domena” to także zabezpieczenia DNSSEC czy DNS over TLS. Z pewnością warto, aby podobne standardy bezpieczeństwa, które od lat funkcjonują w nazwa.pl, zostały wdrożone przez innych partnerów NASK.

OVH SAS

Miniony rok w segmencie nazw domeny .pl był dla OVHcloud niezwykle satysfakcjonujący. Patrząc zaś z szerszej perspektywy – dobre wyniki sprzedaży domen odzwierciedlają solidną kondycję projektów on-line. Cyfrowy biznes trzyma się mocno, e-projektów przybywa, co napędza popyt i inwestowanie w nowe domeny przez użytkowników.

W 2023 roku odnowienia w OVHcloud utrzymywały się na stabilnym poziomie, zaś wskaźnik ten został doceniony przez NASK, który podczas dorocznej konferencji dla Partnerów przyznał OVHcloud wyróżnienie za pierwsze miejsce w liczbie odnowień domen „.pl”.

Ucieszył nas ponadto fakt, że OVHcloud znalazł się w pierwszej trójce rejestratorów nowych domen w kraju. Powyższą pozycję będziemy się starali utrzymać, gdyż zdajemy sobie sprawę, że dla większości abonentów stron w Polsce domena z końcówką „.pl” jest elementem pozycjonowania firmy, określającej tożsamość. Ponadto domeny z rozszerzeniem .pl niezmiennie pozostają bestsellerem, są tradycyjnie pierwszym wyborem wielu użytkowników. Nad Wisłą przyjęło się, że to właśnie .pl zapewnia najlepszą rozpoznawalność. Nie ma w tym nic dziwnego, w końcu funkcjonuje już od ponad trzech dekad i wpisała się w świadomość użytkowników na tyle mocno, że firmy tu działające decydują się na nazwy właśnie z polską końcówką.

Ponadto w naszej ocenie rosnący rynek on-line wpływa też, co obserwujemy, na potrzebę zapewnienia stabilności i zabezpieczenia cyfrowych projektów. Użytkownicy szukają bezpiecznych rozwiązań, stąd niezmiennie będziemy się koncentrować na zapewnianiu najlepszych jakościowo usług w segmencie domen, jak i pozostałych produktów z naszego portfolio, w tym chmury publicznej.

PERSKIMEDIA Szymon Perski



W minionym roku nasze obserwacje potwierdziły, że kluczowym aspektem naszej oferty nie jest cena, ale raczej wysoki poziom wsparcia technicznego, skupienie się na indywidualnych potrzebach naszych użytkowników oraz niezmienna jakość świadczonych usług. Zauważyliśmy również wzrost liczby przypadków nadużyć związanych z wykorzystaniem domen krajowych. Ponadto, obserwujemy zwiększone zainteresowanie nabywaniem domen zagranicznych, szczególnie europejskich oraz gTLD. W naszym portfolio, które liczy ponad 115 tysięcy domen, te zagraniczne stanowią 17% w stosunku do 15% z poprzedniego roku. Przed nami kolejny rok wyzwań, w którym jednym z nich z pewnością będzie zintensyfikowanie działań prewencyjnych przeciwko wykorzystywaniu adresów internetowych rejestrowanych w naszym serwisie do celów niezgodnych z prawem.

DOMENY.TV MSERWIS Sp. z o.o.



W 2023 roku odnotowaliśmy znaczny, ponaddwukrotny wzrost liczby rejestracji nazw domen .pl w naszym serwisie w porównaniu z rokiem 2022.

Naszym zdaniem miało na to wpływ co najmniej kilka czynników. Najważniejszy to poprawiające się otoczenie gospodarcze. Malejąca dynamika inflacji sprawiła, że nasi klienci zaczęli patrzeć w przyszłość z większym optymizmem. Przełożyło się to na dużą liczbę rejestracji nazw domen pod nowe projekty, jak również mniejszy wskaźnik rezygnacji z odnowień niż w roku poprzedzającym.

Choć jest jednym z prawie 1100 rozszerzeń oferowanych w naszym serwisie Domeny.tv, w których można zarejestrować własną nazwę domeny, domena .pl jest niekwestionowanym liderem, jeśli chodzi o liczbę dokonanych rejestracji w Polsce. Jest to niezmiennie pierwszy wybór, jeśli chodzi o końcówkę domenową dla projektów skierowanych na polski rynek. Często, jeśli inne rozszerzenie jest wybierane jako główny adres projektu, nazwa w domenie .pl jest rejestrowana równoległe w celu zabezpieczenia marki.

Ważnym aspektem jest regularna edukacja abonentów domen. Od kilku lat przykładamy szczególną uwagę do tematyki nazewnictwa. Dla strategii biznesu niezmiennie istotny jest wybór odpowiedniej nazwy, jak i rozszerzenia domeny. Przekazujemy wiedzę naszym odbiorcom w formie artykułów na blogu, czy też e-booka namingowego, jak podjąć właściwe decyzje w tym zakresie.

Edukujemy również klientów w zakresie bezpieczeństwa, gdzie efekt widzimy między innymi w postaci coraz powszechniejszego użycia DNSSEC, utrzymywania pełnych i aktualnych danych kontaktowych oraz zabezpieczania dostępu do panelu domeny aplikacją 2FA lub kluczem sprzętowym. Ważnym elementem jest też współpraca z NASK mająca na celu szybkie wykrywanie i reagowanie na incydenty, przykładowo związane z używaniem nazw domen w celach phishingowych. W interesie całego rynku jest to, aby nasi klienci mieli jak największą świadomość korzyści oraz możliwości, jakie niesie użytkowanie własnej nazwy w domenie .pl. Daje to łącznie większe prawdopodobieństwo odnowienia usługi domenowej w kolejnych latach.

LH.pl Sp. z o.o.



W LH.pl w 2023 roku obserwowaliśmy zdecydowane zwiększenie zainteresowania klientów usługami domenowymi i hostingowymi po dość wymagającym 2022 z powodu wybuchu wojny. Firmy chętniej wykupują więcej rozszerzeń domen oraz decydują się na większe pakiety hostingowe. Do naszych sukcesów w zeszłym roku można zaliczyć także pozytywną certyfikację ISO 9001 oraz 27001 jako potwierdzenie jakości oraz wysokiego poziomu bezpieczeństwa.

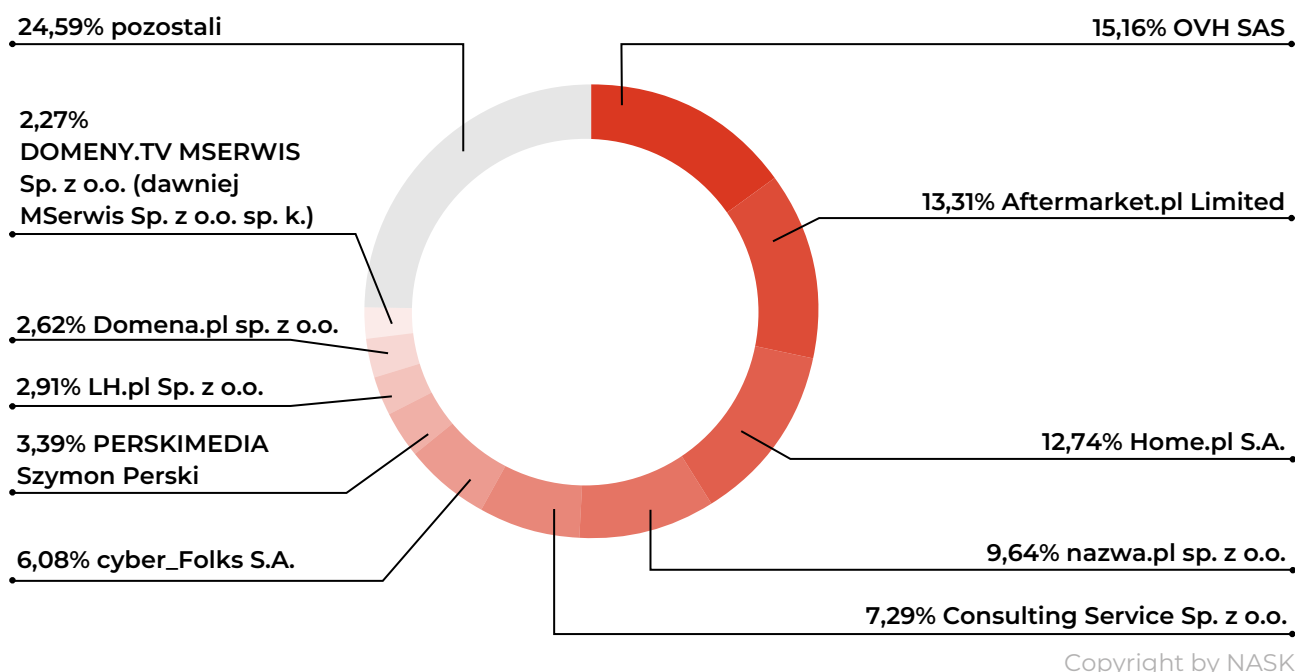
Niemniej jednak 2023 przyniósł także liczne wyzwania. Podobnie jak inne firmy, odnotowaliśmy wzrost kosztów prowadzenia działalności, głównie na skutek podwyżek płac oraz energii. Postawiono przed rejestratorami domen oraz firmami hostingowymi liczne obowiązki legislacyjne: DSA (Akt o usługach cyfrowych), zarys NIS2 (Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii), Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej. Czeką nas także nieuchronnie implementacja Prawa komunikacji elektronicznej, która także nałoży dodatkowe obowiązki.

W 2023 nasz dział bezpieczeństwa zauważył zwiększoną liczbę ataków cybernetycznych, np. phishing – coraz więcej domen .pl jest rejestrowanych z przeznaczeniem na przeprowadzanie phishingu. Wdrożyliśmy rozwiązania, które minimalizują ryzyka z tym związane.

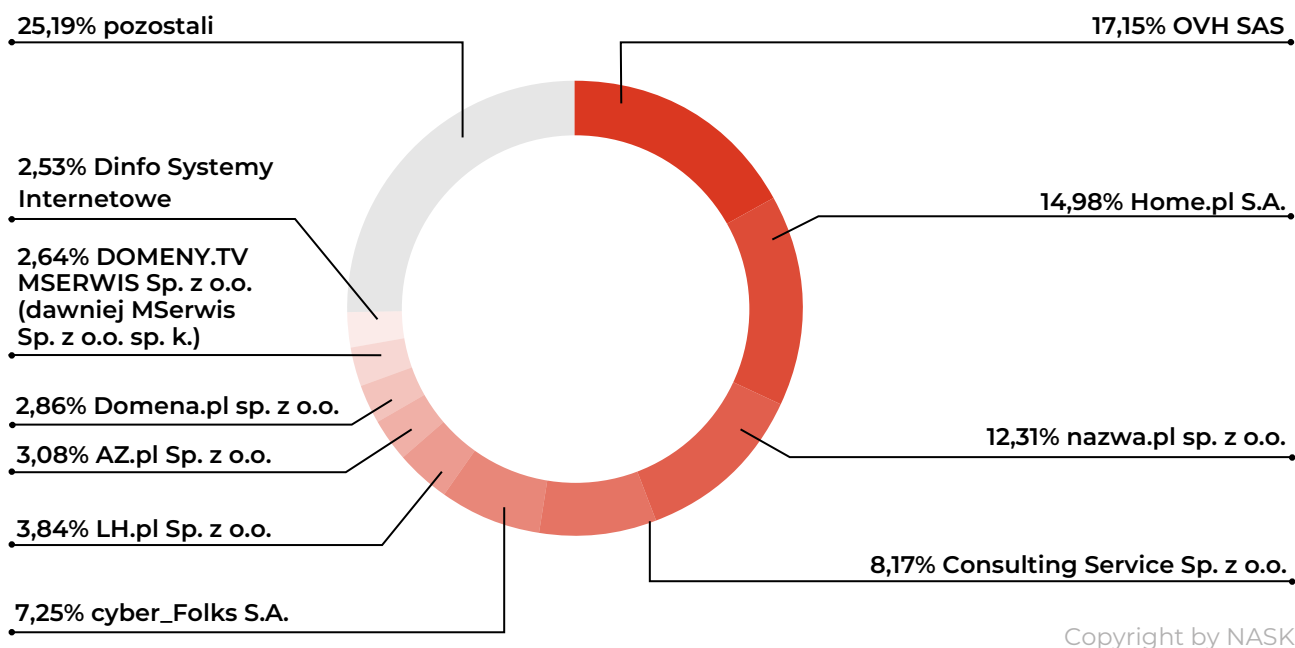
Mimo tych wyzwań mogę potwierdzić, że jesteśmy zadowoleni z wyników i cieszy nas fakt, że nasze rozwiązania przyciągają coraz większą rzeszę klientów. Jesteśmy gotowi na dalszy rozwój i podejmowanie kolejnych wyzwań, aby realizować naszą misję zapewniania klientom ciągłości działania w Internecie.

Podział rynku nazw domeny .pl

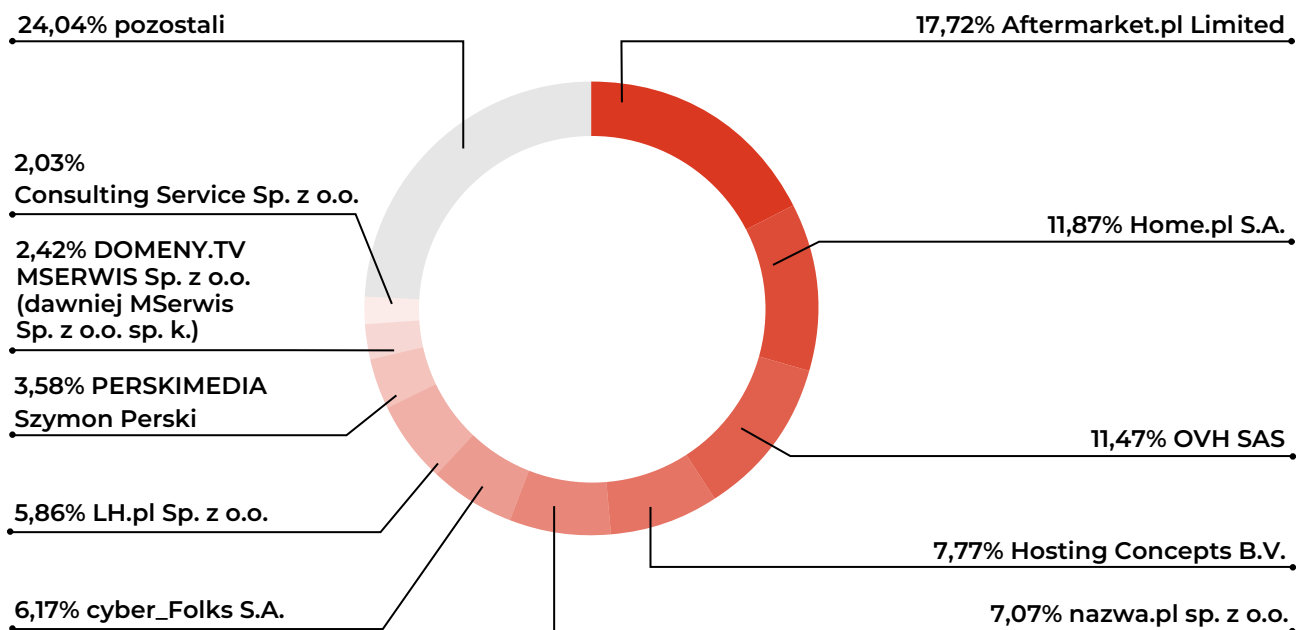
Procentowy udział Partnerów w obsłudze nazw domeny .pl, 2023



Procentowy udział Partnerów w obsłudze Abonentów nazw domeny .pl, 2023

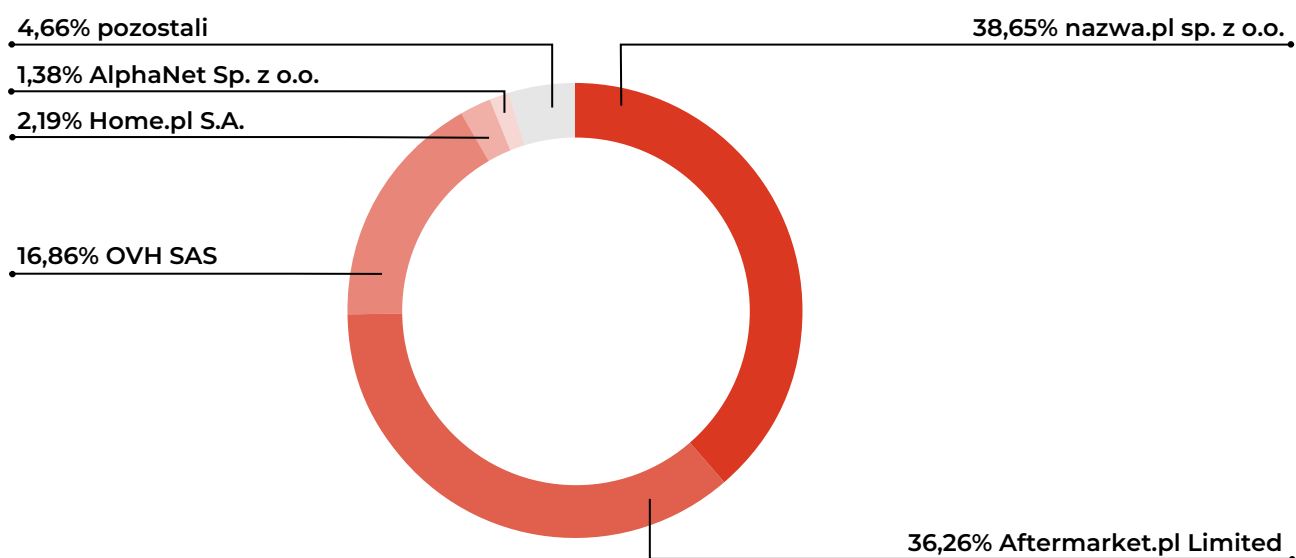


Procentowy udział Partnerów w rejestracjach nazw domeny .pl, 2023



Copyright by NASK

Udział Partnerów w obsłudze nazw domeny .pl zabezpieczonych DNSSEC, 2023



Copyright by NASK



CZĘŚĆ II

Internet oczami ekspertów z branży DNS

Informacje o badaniu

Prezentujemy Państwu **wykonane po raz pierwszy** badanie eksperckie. O opinie dotyczące Internetu, w pięciu kluczowych obszarach (Popularność e-usług, Zagrożenia w sieci, Nienawiść w Internecie, Bezpieczeństwo cyfrowe klientów, Rynek i promocja on-line) zapytaliśmy rejestratorów – naszych partnerów biznesowych, współpracujących z NASK-PIB w ramach Programu Partnerskiego. Jego celem było poznanie opinii ekspertów zajmujących się Internetem, na temat rozwoju technologicznego Polski, użytkowania Internetu, zagrożeń występujących w sieci oraz tego, jak Internet pomaga w prowadzeniu firm. W badaniu wzięło udział 15 przedsiębiorców. Dobór przedstawicieli tej branży był celowy, z uwagi na charakter ekspercki badania. Wyniki pozwolą w przyszłości na porównanie pozyskanej wiedzy i opinii ekspertów z opiniami reprezentatywnej grupy Polaków – użytkowników sieci. W kolejnych edycjach raportu planujemy zaprezentować Państwu także wyniki ilościowego badania na Polakach. Tymczasem mamy nadzieję, że nasze pierwsze badanie eksperckie dostarczy Państwu ciekawych informacji. Serdecznie zachęcamy do lektury!

METODOLOGIA BADANIA

Badania on-line (CAWI) na partnerach biznesowych (rejestratorach) NASK-PIB.

CZAS TRWANIA ANKIETY: 20 minut

REALIZACJA BADANIA: 17.01–29.02.2024

Pytania badawcze

1. Która z e-usług była wykorzystywana w Polsce najczęściej w ciągu ostatnich 12 miesięcy?
2. Które z e-identyfikacji były wykorzystywane najczęściej podczas korzystania z usług on-line?
3. Jak oceniana jest Polska pod względem rozwoju i wprowadzania e-usług w sektorze publicznym, w porównaniu z innymi krajami Unii Europejskiej?
4. Które z obecnych zagrożeń związanych z rozwojem technologii wywołują największe obawy?
5. Która z przeglądarek internetowych używana jest najczęściej?
6. Jak często można spotkać się z agresją on-line lub negatywnymi bądź obraźliwymi komentarzami w sieci?
7. Jaka forma agresji w Internecie jest najbardziej powszechna i jakie są jej motywy?
8. Jak najczęściej zabezpieczane są e-usługi w Polsce?
9. Jakie dane służą rejestratorom do weryfikacji informacji o kliencie?
10. Jakie formy reklamy i promocji są najczęściej stosowane w Internecie w branży domenowej?

Wnioski z badania

1. Bankowość internetowa, zakupy on-line i cyfrowa komunikacja są kluczowymi obszarami, w których technologia zyskuje na znaczeniu w codziennym życiu.
2. Do e-identyfikacji najczęściej wykorzystywany jest profil zaufany, ePUAP oraz aplikacja mObywatel.
3. Polska uzyskała pozytywną ocenę pod względem rozwoju i wprowadzania e-usług w sektorze publicznym, w porównaniu z innymi krajami Unii Europejskiej.
4. Najbardziej dominującymi e-usługami administracji publicznej są: podatki.gov.pl i ePUAP.
5. Kradzież tożsamości cyfrowej oraz dezinformacja są obecnie kluczowymi zagrożeniami w cyberprzestrzeni.
6. Agresja jest obecna w różnych obszarach Internetu, ale najbardziej w mediach społecznościowych.
7. Źródłem konfliktów on-line są najczęściej kwestie polityczne.
8. Firmy, aby edukować swoich klientów w zakresie zagrożeń w sieci, stosują różnorodne strategie komunikacyjne.
9. Realnym zagrożeniem dla firm staje się phishing.
10. Do najczęściej stosowanych promocji należą rabaty na rejestrację i programy partnerskie.



Popularność e-usług

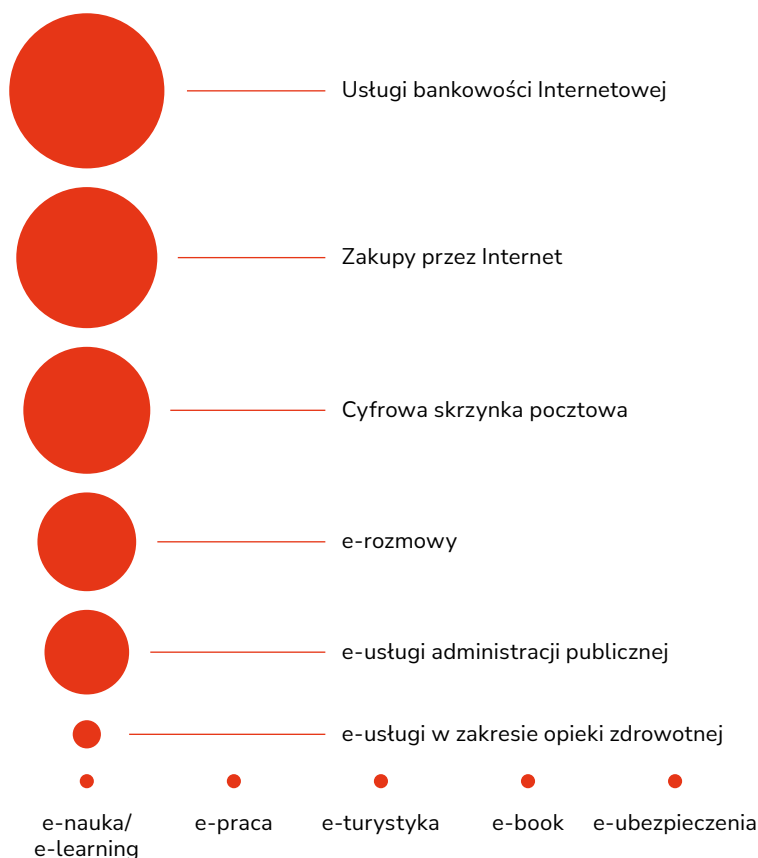
Do czego potrzebny nam Internet?

Usługa bankowości internetowej była wybierana najczęściej (11 na 15 odpowiedzi), co sugeruje, że korzystanie z platform bankowych on-line stało się nieodłącznym elementem codzienności. Niewiele mniej popularne są zakupy przez Internet (10), co potwierdza rosnącą tendencję do preferowania wygody zakupów on-line.

Niezmiennie popularna jest cyfrowa skrzynka pocztowa (9) oraz e-rozmowy (czaty, komunikatory itp. – 7).

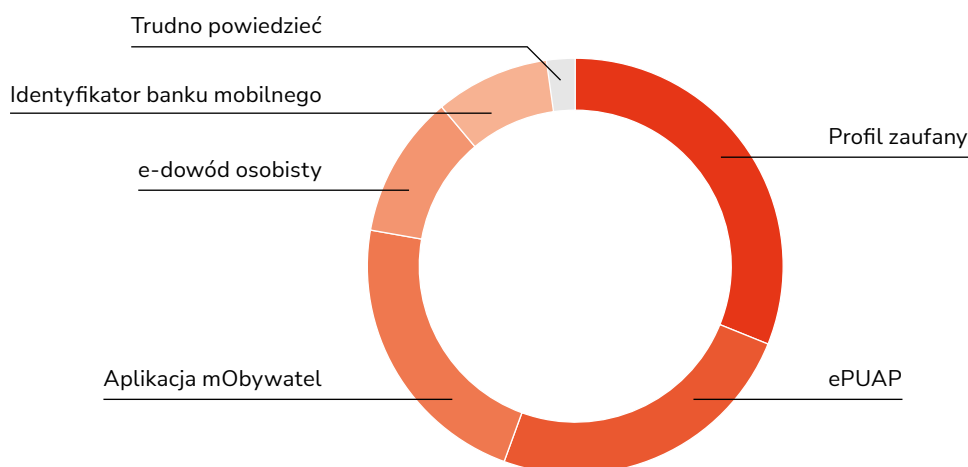
Badani przez nas eksperci są także zainteresowani korzystaniem z e-usług administracji publicznej (6), ale już niechętnie zwracają się w stronę usług e-opieki/e-usług w zakresie opieki zdrowotnej (2). Zainteresowaniem badanych nie cieszyły się także e-nauka/e-learning oraz poszukiwanie pracy on-line.

✘ Która z poniższych e-usług była Pana/Pani zdaniem najczęściej wykorzystywana w Polsce, w ciągu ostatnich 12 miesięcy?



Podczas korzystania z e-usług badani chętnie używają różnych e-identyfikacji. Do najpopularniejszych z nich należą profil zaufany (14 odpowiedzi), ePUAP (11) oraz aplikacja mObywatel (10). Niektórzy korzystają z mniej popularnego e-dowodu osobistego (5) oraz z identyfikatora banku mobilnego (4).

✂ Czy w ciągu ostatnich 12 miesięcy korzystał(a) Pan/Pani z którejkolwiek z poniższych e-identyfikacji podczas korzystania z jakichś usług on-line?



Copyright by NASK

W parze z praktycznym wykorzystaniem e-identyfikacji idzie także pozytywna ocena Polski pod względem rozwoju i wprowadzania e-usług w sektorze publicznym, w porównaniu z innymi krajami Unii Europejskiej. 8 na 15 badanych przez nas ekspertów uważa, że sytuacja Polski jest lepsza bądź zdecydowanie lepsza od innych państw UE. Co więcej, żaden z respondentów nie uważa, że Polska rozwija się gorzej od innych europejskich krajów, a 2 ocenia jej rozwój na tym samym poziomie co innych porównywanych krajów. Dość duża grupa (5 wskazań) nie umiała zająć stanowiska w tej sprawie. W szczególności badani wskazali na e-usługi administracji publicznej, jak podatki.gov.pl i ePUAP, jako te, które najbardziej dominują w rozwoju nad innymi krajami UE (7). Na drugim miejscu plasują się usługi bankowości internetowej (5), co ponownie potwierdza rosnącą popularność korzystania z bankowości on-line w Polsce. Słabiej, jeśli chodzi o rozwój Polski na tle innych krajów Unii Europejskiej, oceniane są e-commerce, usługi e-opieki (w tym e-recepty), e-turystyka (1) oraz e-usługi związane z nauką, pracą, rozmowami, e-bookami, ubezpieczeniami i kulturą (0).

Bankowość internetowa, zakupy on-line i cyfrowa komunikacja są kluczowymi obszarami, gdzie technologia zyskuje na znaczeniu w codziennym życiu, co może być wynikiem zarówno ułatwień dostępnych dla klientów, jak i trendów cyfrowych.

Preferowanie zakupów on-line świadczy o zaufaniu do platform e-commerce i łatwości dokonywania transakcji przez Internet. Niewątpliwie do popularności tej e-usługi przyczyniła się także pandemia SARS-CoV-2. Może dziwić fakt, że po zmianach

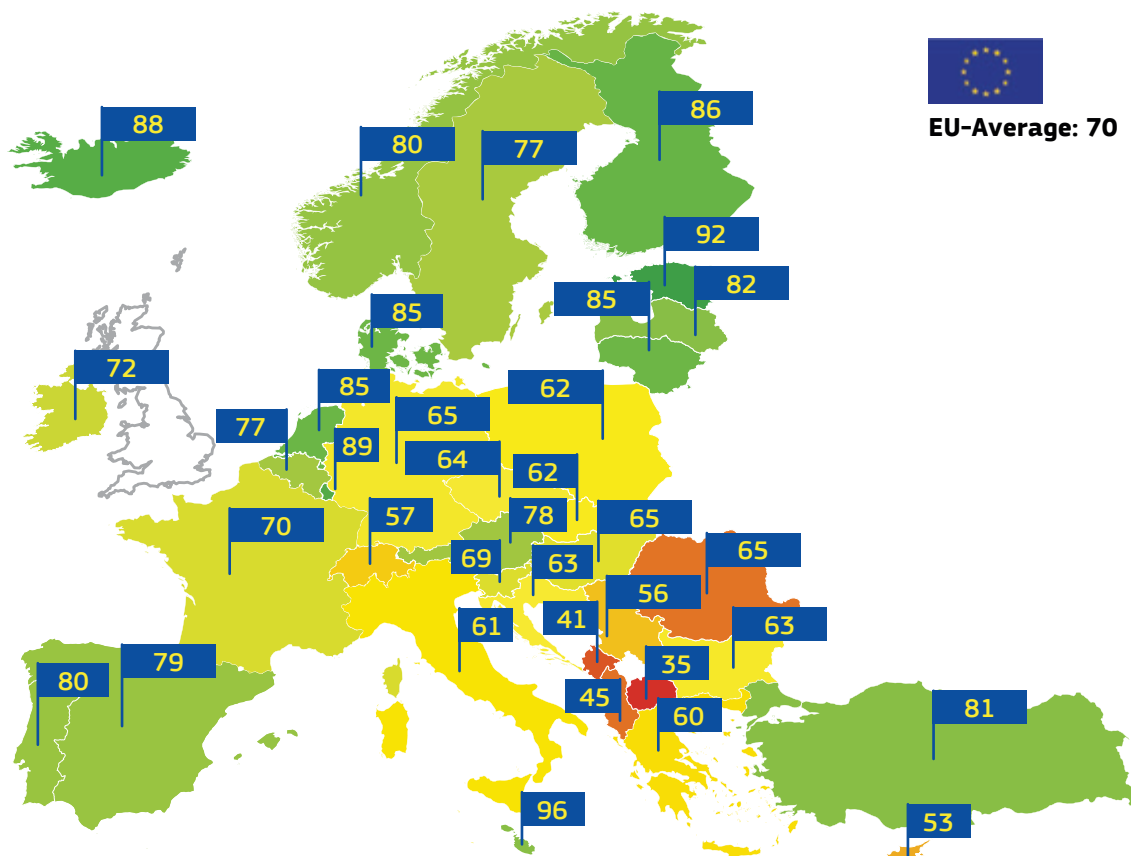
jakie zaszły w sektorze opieki zdrowotnej po pandemii, zainteresowanie wśród badanej grupy korzystaniem z usług e-opieki jest bardzo niskie. Niechęć wśród badanych wzbudza również e-nauka/e-learning oraz poszukiwanie pracy on-line. Prawdopodobnie dlatego, że są to osoby o ustabilizowanej już sytuacji zawodowej oraz określonym wykształceniu. Brak zainteresowania widoczny był również w zakresie: e-booków, e-ubezpieczenia, e-turystyki oraz e-kultury. Co ciekawe żaden z respondentów nie zadeklarował, że nie korzysta z żadnej formy e-identyfikacji. Może to wskazywać na rosnącą świadomość i akceptację konieczności korzystania z tego rodzaju rozwiązań,

szczególnie w tym szczególnym środowisku, co wpływa także na wybór konkretnej formy identyfikacji przez użytkowników.

Pozytywna, w opinii badanych przez nas ekspertów, ocena Polski pod względem rozwoju i wprowadzania e-usług w sektorze publicznym na tle innych krajów UE może sugerować, że Polska skoncentrowała się na rozwijaniu cyfrowych usług publicznych, co zdaje się być zauważone przez ankietowanych. Badani dobrze oceniają działania państwowe w tym obszarze oraz istnieje duże zainteresowanie i aktywność badanych w korzystaniu z usług on-line dostarczanych przez instytucje publiczne.

Według badania przeprowadzonego przez Komisję Europejską poziom rozwoju e-usług w Polsce plasuje się poniżej unijnej średniej.

✂ Poziom rozwoju e-usług w Unii Europejskiej



Poziom rozwoju poszczególnych krajów oceniono na podstawie badania czterech wymiarów:

- » nastawienie na użytkownika (Na jakim poziomie są świadczone usługi on-line? Jak przyjazne są one dla urządzeń mobilnych? Jakie są dostępne mechanizmy wsparcia i opinii on-line?)
- » przejrzystość (Czy administracje publiczne zapewniają klarowne, otwarcie komunikowane informacje na temat sposobu świadczenia swoich usług? Czy są transparentne w kwestii tworzenia polityki i procesów projektowania usług cyfrowych, jak również w sposobie przetwarzania danych osobowych użytkowników?)
- » kluczowe udogodnienia (Jakie technologiczne udogodnienia są dostępne dla świadczenia usług eGovernment?)
- » usługi transgraniczne (Jak łatwo obywatele z zagranicy mogą uzyskać dostęp i korzystać z usług on-line? Jakie mechanizmy wsparcia i opinii on-line są dostępne dla użytkowników transgranicznych?).

Otrzymany wynik mieści się w zakresie od 0 do 100 punktów.

KOMENTARZ EKSPERTA

Cyfryzacja usług w Polsce pomimo relatywnie niskiego poziomu w porównaniu do innych krajów europejskich, ulega ciągłej poprawie. Dynamika zachodzących zmian daje nadzieję, że w perspektywie kilku lat poziom cyfryzacji usług będzie na poziomie porównywalnym z innymi krajami UE.

Istotną rolę w przyspieszeniu tego procesu odegrała pandemia COVID-19 oraz fakt rosnącej społecznej dostępności do Internetu. W porównaniu do roku 2015, w 2022 roku na 1000 mieszkańców Polski 870 osób było użytkownikami Internetu (w 2015 roku zaledwie 680). Pod względem liczby abonentów telefonii mobilnej na 1000 mieszkańców Polacy zajmują IV miejsce w Europie (po Estonii,

Litwie i Włoszech). Krajem przodującym pod względem liczby abonentów telefonii mobilnej na 1000 mieszkańców jest Japonia (1675 abonentów na 1000 mieszkańców), a w Polsce wskaźnik ten wynosi 1320 [Rocznik Statystyki Międzynarodowej, 2023, GUS, Warszawa 2023].

Dostępność do Internetu, w tym do szerokopasmowego łącza powoduje, że Polacy częściej korzystają z bankowości internetowej, częściej dokonują zakupów przez Internet czy korzystają z różnego rodzaju systemów komunikacji internetowej. Chęć załatwiania spraw przez Internet wpływa również na rosnącą skalę korzystania z różnych e-identyfikacji gwarantujących poczucie bezpieczeństwa.

Prof. dr hab. inż. Joanna Ejdys

POLITECHNIKA BIAŁOSTOCKA, WYDZIAŁ INŻYNIERII ZARZĄDZANIA

e-rozmowy e-puap

e-biznes e-opieka

e-commerce

e-ubezpieczenia e-mail e-book

e-kultura

e-bankowość e-dowód osobisty

e-biznes

e-identyfikacja

e-administracja

e-turystyka e-płatności

e-consulting

e-recepty e-usługa

e-learning



Zagrożenia w sieci

Czego boimy się najbardziej?

Zagrożenia cyberbezpieczeństwa to kolejny obszar, w którym chcieliśmy poznać opinie naszych ekspertów. Analizując wyniki badań dotyczące obaw związanych z różnymi zagrożeniami, można wyróżnić kilka istotnych trendów:

- **WYSOKA ŚWIADOMOŚĆ DEZINFORMACJI** (11 wskazań). Obawy związane z dezinformacją wskazują na rosnące zrozumienie tego, jak istotną rolę odgrywa cyberprzestrzeń w manipulowaniu informacjami.
- **PROBLEMY ZWIĄZANE Z DOSTĘPEM DO INTERNETU** także wywołują obawy wśród badanych (9). Jest to zrozumiałe, ponieważ wiele aspektów codziennego życia, zarówno prywatnego, jak i zawodowego, zależy od dostępu do sieci.
- **ZAGROŻENIA CYBERATAKAMI I ATAKAMI NA INFRASTRUKTURĘ KRYTYCZNĄ**. Obawy związane z cyberatakami na Polskę oraz wyłączeniem podstawowych systemów infrastrukturalnych (6) są zgodne z globalnym trendem zwiększającej się aktywności cyberprzestępczej i cyberwojennej.
- **WYKRADANIE DANYCH OSOBOWYCH**. Obawy związane z wykradaniem danych osobowych (6) podkreślają, że ochrona prywatności staje się nieustannie ważnym aspektem cyberbezpieczeństwa.
- **PRZERWANIE ŁAŃCUCHA DOSTAW I WOJNA HYBRYDOWA**. Obawy związane z przerwaniem łańcucha dostaw produktów spożywczych (6) i zagrożeniem wojny hybrydowej (4) podkreślają, że cyberbezpieczeństwo jest ściśle powiązane z bezpieczeństwem narodowym i globalnym łańcuchem dostaw.
- **ZAINFEKOWANIE URZĄDZEŃ ZŁOŚLIWYM OPROGRAMOWANIEM** (3). Zagrożenie to wzbudza mniej niepokoju wśród badanych, gdyż prawdopodobnie wiedzą, jak się przed nim bronić.

Najmniej niepokoju wzbudza zablokowanie działania łączności handlowej, zakłócenia w funkcjonowaniu komunikacji np. pociągi, samoloty, autobusy, czy działania państw trzecich na kraj (1). Żaden z badanych nie wskazał zablokowania działania sieci przekazów bankowych oraz rynku akcji i obligacji jako potencjalne zagrożenie z obszaru cyberbezpieczeństwa.

Jednocześnie badani wskazują, że **kradzież tożsamości cyfrowej** jest jednym z kluczowych obecnie zagrożeń (14 wskazań). To potwierdza rosnącą świadomość społeczeństwa na temat poważnych konsekwencji, jakie może przynieść utrata tożsamości cyfrowej. Nikt z respondentów nie odpowiedział „Nie” ani „Zdecydowanie nie”.

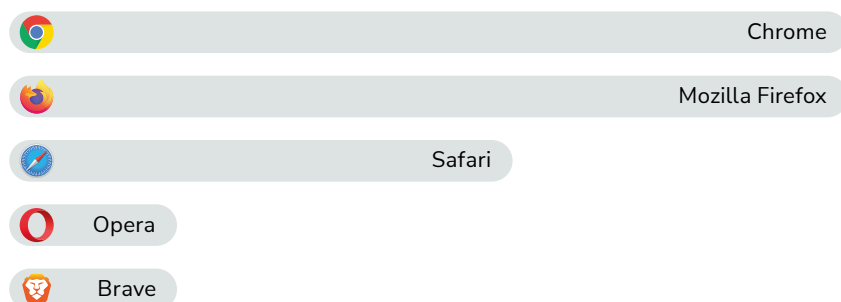
✂ Których z poniżej wymienionych zagrożeń obawiasz się najbardziej?



Copyright by NASK

Zapytaliśmy naszych badanych także o to, której przeglądarki używają najczęściej. Na pierwszym miejscu (po 5 wskazań) plasują się Chrome i Mozilla Firefox, następnie przeznaczona głównie dla użytkowników głównie systemów Apple przeglądarka Safari (3) i na trzecim miejscu Opera i Brave (po 1). Warto zauważyć, że żaden z respondentów nie wskazał przeglądarki Microsoft Edge ani Tor jako swojej najczęściej używanej.

✂ Której przeglądarki używa Pan(i) najczęściej?



Copyright by NASK

W kontekście cyberbezpieczeństwa na świecie, wyniki ankiety ukazują kompleksowe spojrzenie na różne aspekty zagrożeń. Wzrost świadomości w obszarze dezinformacji, ataków cybernetycznych i bezpieczeństwa infrastruktury

krytycznej wymaga globalnej współpracy i stałego dostosowywania strategii, aby skutecznie przeciwdziałać ewoluującym zagrożeniom w cyberprzestrzeni. W miarę postępu technologicznego i rosnącej liczby

platform internetowych, walka z dezinformacją staje się kluczowym wyzwaniem dla cyberbezpieczeństwa na świecie. Ostatnie badania przeprowadzone przez Fundację Digital Poland i organizację fact-checkingową Demagog pt.: *Dezinformacja oczami Polaków (Warszawa 2024)* potwierdzają, że poziom dezinformacji w Polsce utrzymuje się na bardzo wysokim poziomie.

Bezpieczeństwo sieci staje się obecnie fundamentalnym aspektem utrzymania stabilności i integralności społeczeństwa, a bezpieczeństwo infrastruktury krytycznej, takiej jak dostawa energii, wody czy ciepła, staje się priorytetem

na arenie międzynarodowej. Wiele aspektów codziennego życia, zarówno prywatnego, jak i zawodowego, zależy od dostępu do sieci. Ponadto dostęp do Internetu to nie tylko wygoda, ale również kluczowe narzędzie komunikacji, edukacji i dostępu do informacji. Dochodzi tutaj również kwestia ochrony prywatności w cyberprzestrzeni. Kradzież tożsamości cyfrowej jest jednym z kluczowych obecnie zagrożeń. To potwierdza rosnącą świadomość społeczeństwa na temat poważnych konsekwencji, jakie może przynieść utrata tej tożsamości. Ochrona tożsamości on-line staje się priorytetem, a działania na rzecz poprawy cyberbezpieczeństwa i edukacji w tym zakresie są kluczowe dla społeczeństwa.

KOMENTARZ EKSPERTA

Badania dotyczące opinii ekspertów pionu domen NASK, przeprowadzone w ramach 15 firm na temat zagrożeń w sieci, to kolejna interesująca perspektywa przedstawiająca występujące trendy w tym obszarze. Wyniki wyraźnie wskazują, że świadomość istnienia określonych zagrożeń płynących ze strony sieci w opinii ekspertów istnieje (wielce niepokojącą sytuacją byłoby, gdyby tak się nie stało). Interesująca wydaje się być jednak gradacja tych zagrożeń. Obawy ekspertów budzi bowiem w pierwszej kolejności dezinformacja (dużo się o niej ostatnio pisze i mówi w związku z minioną pandemią COVID-19 i konfliktem zbrojnym za wschodnią granicą), w drugiej kolejności brak dostępu do Internetu, następnie *ex aequo* wyłączenie podstawowych systemów (energia elektryczna, gaz, ciepło, blokada linii i sieci telefonicznych oraz transmisji danych), przerwanie łańcucha dostaw produktów spożywczych i wykradanie danych osobowych, co ciekawe zablokowanie działania sieci przekazów bankowych oraz rynku akcji i obligacji nie zostało zaznaczone przez żadnego z respondentów.

Natomiast kradzież tożsamości cyfrowej zdecydowanie postrzegana jest jako kluczowe zagrożenie. Bo takim w rzeczywistości jest. Wśród najczęściej używanych przez respondentów przeglądarek wskazywana była Chrome, Mozilla Firefox, następnie Safari (dotyczy użytkowników Mac), na Operę wskazała jedna osoba, natomiast Tor i Microsoft Edge nie został wskazany przez żadną z osób. Bardzo interesujące badania i ich wyniki. Polecam lekturę całego raportu. Warto podobne badania przeprowadzić wśród szerszego grona użytkowników nie będących ekspertami (ze specyfikacją na podstawowe dane metryczkowe: m.in. wiek, płeć, wykształcenie, wykonywany zawód, pełnioną rolę w strukturze instytucji, firmy etc.) i zestawić ich odpowiedzi ze wskazaniami ekspertów. Na tej podstawie będzie można sformułować rekomendacje dotyczące występujących deficytów oraz wdrożenia koniecznych mechanizmów i programów edukacyjnych niwelujących te deficyty docelowo prowadzących do świadomego, odpowiedzialnego i bezpiecznego korzystania z sieci.

Prof. UWr dr hab. Barbara Wiśniewska-Paź



Nienawiść w Internecie

Agresja jako zjawisko w sieci

Nasi badani rzadko doświadczają agresji w Internecie. W ciągu ostatnich 12 miesięcy doświadczyło jej tylko 4 respondentów, a 1 osoba nie była pewna, czy spotkała się z agresją, czy też nie. Podobnie jest w przypadku agresji w Internecie skierowanej do firm. Twierdząco odpowiedziało jedynie 2 ekspertów, a 3 miało problem z identyfikacją, czy zachowanie skierowane w stronę firmy było agresją czy też nie, co może świadczyć o niepewności w identyfikowaniu lub monitorowaniu ewentualnych negatywnych sytuacji on-line. Jednak aż 13 badanych potwierdziło, że w ciągu ostatnich 12 miesięcy widzieli, żeby ktoś inny stał się ofiarą agresji w Internecie lub napisał w Internecie coś negatywnego lub obraźliwego. Jedynie 1 osoba odpowiedziała negatywnie na to pytanie, a 1 miała problem z właściwą identyfikacją zaobserwowanego zachowania.

Najczęściej była to agresja związana z mową nienawiści (*hate speech*) – 13 wskazań, z *trollingiem* (prowokowanie konfliktów, dezinformacja) – 10 i wyśmiewaniem (*mocking*) – 6. Nieco mniej osób zaobserwowało zjawisko wściekłości internetowej (*on-line outrage*) – 4, dyskryminację (na tle rasowym, religijnym, seksualnym czy innym) – 3, nękanie (*bullying*) i osaczanie (*dogpiling*) – 2 oraz wykraczanie poza prywatność (*doxxing*) – 1.

✂ Jakiego rodzaju agresja w Internecie jest Pan(i) zdaniem najczęstsza?

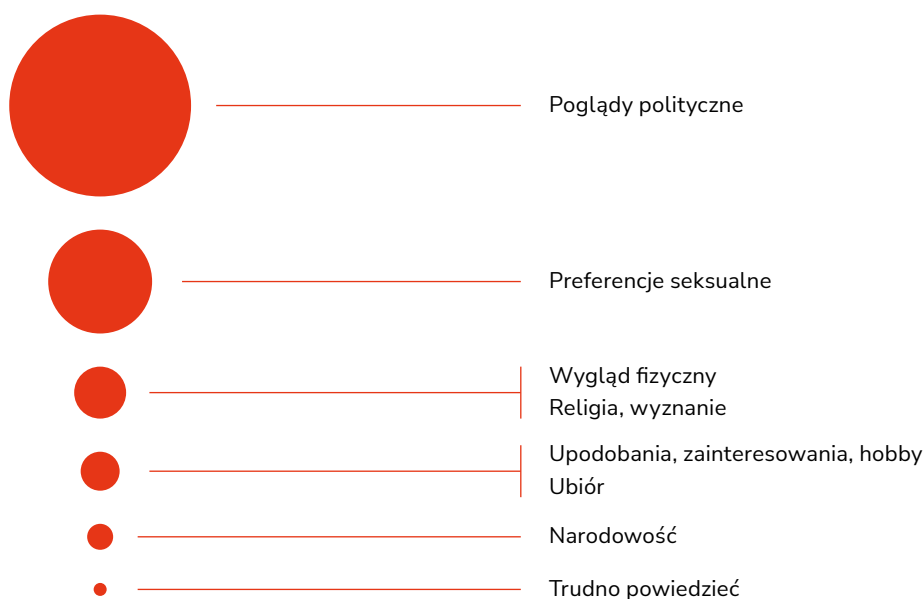


Copyright by NASK

Jako przyczynę agresji badani wskazali poglądy polityczne (14 z 15). Nieco mniej wskazań (8) miały preferencje seksualne oraz wygląd fizyczny

i wyznawana religia (4). To podkreśla różnorodność dziedzin, w których dochodzi do agresji on-line. Czasami wskazywanym powodem są także upodobania, zainteresowania, hobby, narodowość (3), czy styl ubierania się (2). Co ciekawe, brak wskazań dotyczących płci czy koloru skóry. To może wskazywać na postęp w zakresie społecznej świadomości i akceptacji różnic w tych obszarach.

❖ Co Pan(i) zdaniem jest najczęstszym powodem agresji w Internecie?



Copyright by NASK

Zdaniem badanych najczęściej agresji w Internecie można doświadczyć w mediach społecznościowych, jak Facebook, Instagram i YouTube (12 wskazań), na portalach internetowych, jak Onet, WP czy Interia (4), komunikatorach, jak Messenger czy WhatsApp (2), grach on-line oraz w komentarzach pod wiadomościami na portalach informacyjnych (1). Według naszych respondentów najczęściej z agresją można spotkać się na takich portalach jak Facebook – 9 odpowiedzi, X (twitter) – 5, YouTube – 4, Instagram, Tik Tok i Wykop.pl – 2, oraz Twitch – 1. Wśród komunikatorów najczęściej wskazany był Messenger platformy Facebook (2 wskazania) oraz Skype, Discord, Telegram, Teams (po 1 odpowiedzi). Ta niewielka liczba wskazań może wynikać z mniejszej publicznej ekspozycji komunikacji prywatnej w porównaniu do interakcji w mediach społecznościowych.

Podobnie jest z portalami internetowymi. Maksymalna liczba wskazań wśród badanych wynosiła 1 i dotyczyła takich portali jak Onet.pl, TVN24.pl, Gazeta.pl, Pudelek.pl, Plotek.pl, TVP.pl. I chociaż widoczne są tu różnice preferencji, ponieważ respondenci podali różne portale informacyjne – zarówno serwisy informacyjne, jak i rozrywkowe, to liczba wskazań jest niewielka.

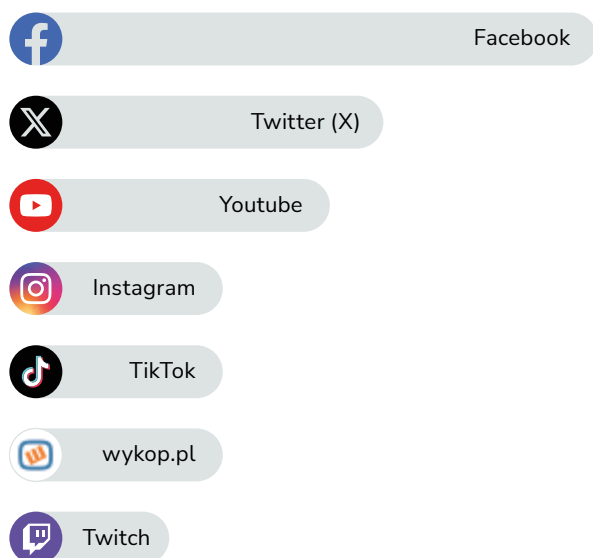
Równocześnie jedynie 6 z badanych przez nas ekspertów nie powstrzymuje się od wyrażania swojej opinii w Internecie z obawy przed staniem się ofiarą agresji cyfrowej, 5 osób powstrzymuje się od komentowania postów w mediach

społecznościowych osób, których nie zna, 4 obawiają się zamieszczania własnych postów w mediach społecznościowych, 3 powstrzymuje się od komentowania postów w grupach w mediach społecznościowych, a 2 powstrzymuje się od komentowania wpisów znajomych w mediach społecznościowych i nie komentuje artykułów/aktualności w mediach społecznościowych.

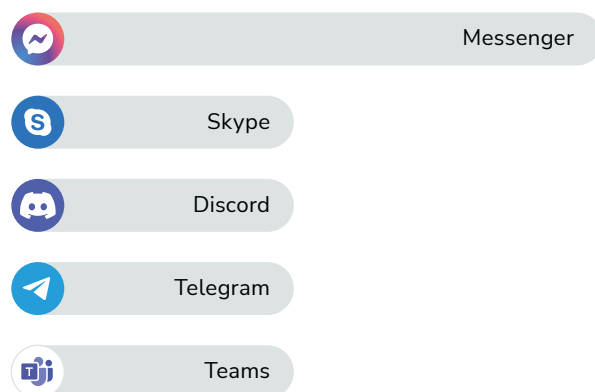
✂ Gdzie w Internecie zauważył(a) Pan(i), że ktoś inny stał się ofiarą agresji w Internecie?



✂ W jakich mediach społecznościowych najczęściej był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji?

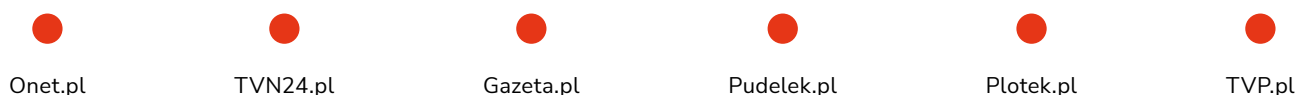


✂ Na jakich komunikatorach najczęściej był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji?



Copyright by NASK

✂ Na jakich portalach internetowych najczęściej był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji?



Copyright by NASK

Można przyjąć założenie, że agresja jest obecna w różnych mediach internetowych, ale jednocześnie może nie być powszechnym zjawiskiem w doświadczeniach respondentów. Warto podkreślić, że wyniki te mogą być subiektywne i zależą od indywidualnych doświadczeń respondentów oraz od tego, które portale są popularne w danej grupie społecznej.

Badani wykazują dość dużą ostrożność wobec nieznanymi. Może to wynikać z obaw związanych z potencjalnymi reakcjami negatywnymi lub agresją ze strony nieznanymi użytkowników. Podobnie jest w przypadku grup w mediach społecznościowych. Ciekawe jest spostrzeżenie dotyczące powstrzymywania się od komentowania wpisów znajomych w mediach społecznościowych, sugerujące, że nawet wśród osób, które zna się osobiście, istnieje pewna obawa przed potencjalną agresją w odpowiedzi na wyrażanie opinii.

Firmy mogą mieć ograniczoną widoczność w tym obszarze lub trudności w śledzeniu komunikatów on-line. Większość firm nie miała żadnych negatywnych doświadczeń, co może wskazywać na to, że większość przedsiębiorstw utrzymuje pozytywną reputację w cyberprzestrzeni i nie doświadcza publicznych ataków czy negatywnych komentarzy.

Wyniki potwierdzają tezę, że kwestie polityczne są często źródłem konfliktów on-line i wskazuje na od dawna już podnoszoną w przestrzeni publicznej ogromną polaryzację społeczeństwa w tym obszarze.

Dominacja Facebooka jako platformy, na której badani obserwowali agresję w Internecie może wskazywać na to, że ta największa sieć społecznościowa jest szczególnie narażona na negatywne interakcje. Tezę tę potwierdza to, że na kolejnych miejscach znalazły się Twitter i YouTube, także znane z szerokiego zasięgu.

KOMENTARZ EKSPERTA

Na obecnym rozwoju technologii świat wirtualny wypiera świat realny. Ludzie w coraz to większym stopniu przenoszą swoją aktywność do Internetu. Dlatego badania życia społecznego realizowanego w świecie wirtualnym jest ważne. Przedstawione wstępne badania eksperckie dotyczące NIENAWIŚCI w Internecie, a szczególnie AGRESJI jako zjawiska w sieci wskazuje, że obawa przed nieuzasadnionymi negatywnymi reakcjami Internautów według tylko 33% badanych nie powoduje blokady w przedstawianiu swoich poglądów. Pozostałe 67% mają wątpliwości i prawdopodobnie ograniczają się w wypowiedziach. Można więc przyjąć, że duża grupa Internautów wręcz rezygnuje z udziału w publicznych dyskusjach z obawy

przed agresją ze strony innych – jest wyłączona z aktywnego udziału w życiu społecznym w Internecie. Warto by zbadać dokładnie, jaka to grupa użytkowników Internetu i czego potrzebują by się nie marginalizować.

Agresja według ekspertów ujawniana jest głównie na społecznościowych forach internetowych. Wskazuje to, że dotychczas wykorzystywane narzędzia eliminacji nienawiści i agresji są nieskuteczne. Konieczne jest szukanie nowych rozwiązań chroniących wolność wypowiedzi i pozwalających włączać się w dyskusję, czyli w życie społeczne dziejące się w Internecie osobom obecnie eliminowanym przez agresję innych.

Dr hab. Bohdan Rożnowski, prof. KUL

KATOLICKI UNIWERSYTET LUBELSKI JANA PAWŁA II, KATEDRA PSYCHOLOGII PRACY, INSTYTUT PSYCHOLOGII

trolling

wyśmiewanie

race

osaczanie

stalking

dezinformacja

dręczenie

hate

dyskryminacja

doxxing

mocking

hate speech

szczucie

cyberbullying

dogpiling

mowa nienawiści

fake news

bullying

trole internetowe

discrimination

on-line outrage

religion

nękanie

disinformation



Bezpieczeństwo cyfrowe klientów

Najpopularniejsze zabezpieczenia e-usług

Zapytaliśmy badanych, czy w trosce o bezpieczeństwo cyfrowe klientów dokonują **analizy ryzyk** dotyczących bezpieczeństwa usług cyfrowych. Większość (10) potwierdziła, że w ich firmie przeprowadzana jest analiza ryzyka dotycząca bezpieczeństwa usług cyfrowych, w 3 firmach nie przeprowadza się takiej analizy, a 2 miały trudności z udzieleniem odpowiedzi na to pytanie. Jest to obszar wymagający uwagi, ponieważ brak takiej analizy może narażać firmę na zagrożenie bezpieczeństwa świadczonych usług czy przetwarzanych danych, ale również na negatywne konsekwencje regulacyjne (np. kary administracyjne). Analiza wyników ankiety dotyczących **zabezpieczeń e-usług** ukazuje, że respondenci podejmują różnorodne i świadome kroki w celu zminimalizowania ryzyk z obszaru cyberbezpieczeństwa. Najbardziej popularne jest wieloetapowe uwierzytelnianie (14 wskazań), cykliczna/regularna aktualizacja oprogramowania (12), firewalle (11), szyfrowanie danych (10) i monitoring systemów (9). Niektóre z badanych przez nas firm korzystają także z systemu wykrywania intruzów (IDS) i systemu zapobiegania włamaniom (IPS) (3).

✂ W jaki sposób najczęściej zabezpiecza Pan(i) swoje e-usługi?



Wieloetapowe uwierzytelnianie



Regularna aktualizacja oprogramowania



Firewalle



Szyfrowanie danych



Monitoring systemów



Systemy wykrywania intruzów



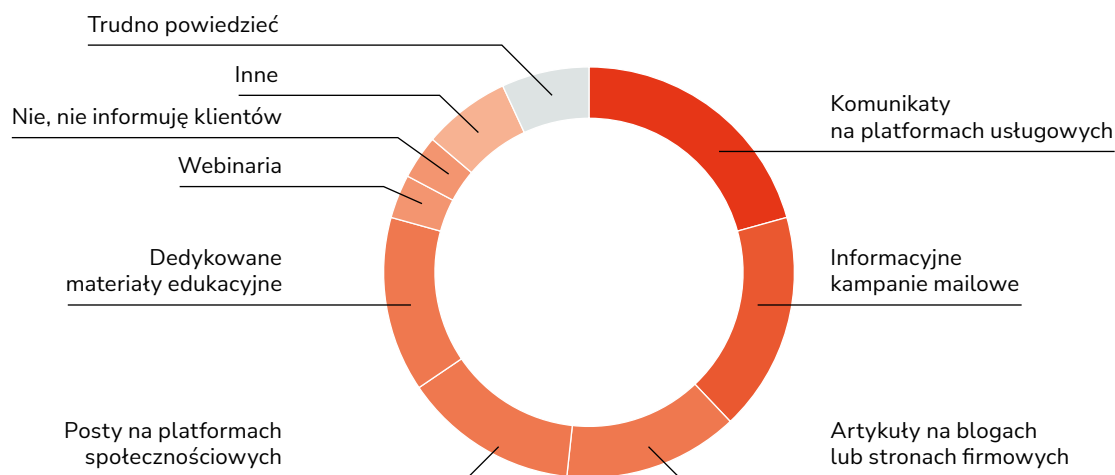
Systemy zapobiegania włamaniom

Copyright by NASK

Równocześnie badani w większości (11 wskazań) nie prowadzą **statystyk dotyczących naruszeń przepisów dotyczących nielegalnego charakteru treści**. Takie statystyki gromadzą jedynie 3 firmy (1 miała problem z odpowiedzią na to pytanie). To może wskazywać, że większość respondentów nie świadczy usług hostingu lub innych, polegających na umożliwianiu klientom końcowym udostępniania treści. 6 z 15 badanych firm potwierdziło, że ich usługi były poddane **phishingowi**. Wskazuje to na pewne doświadczenia i świadomość respondentów w zakresie cyberbezpieczeństwa oraz świadczy o realnym ryzyku

i występowaniu tego rodzaju ataków. 7 ekspertów zadeklarowało, że ich usługi nie były poddane phishingowi, a 2 było trudno udzielić odpowiedzi na to pytanie. W zakresie działań dotyczących poprawy świadomości w obszarze bezpieczeństwa 9 z 15 firm zadeklarowało, że **informuje klientów o zagrożeniach w sieci**, 4 nie podejmuje żadnych tego typu działań, a 2 nie potrafiły udzielić odpowiedzi na to pytanie. Wśród tych dziewięciu firm najczęściej do informowania służą komunikaty na platformach usługowych (6 odpowiedzi), informacyjne kampanie mailowe (5 odpowiedzi), artykuły na blogach lub stronach firmowych (4 odpowiedzi) oraz posty na platformach społecznościowych (4 odpowiedzi). Rzadziej stosowane są materiały edukacyjne i webinaria, rozmowy z klientami oraz bezpośrednio wskazywanie zagrożeń i metod przeciwdziałania im, najczęściej podczas telefonicznych rozmów (po 1 odpowiedzi).

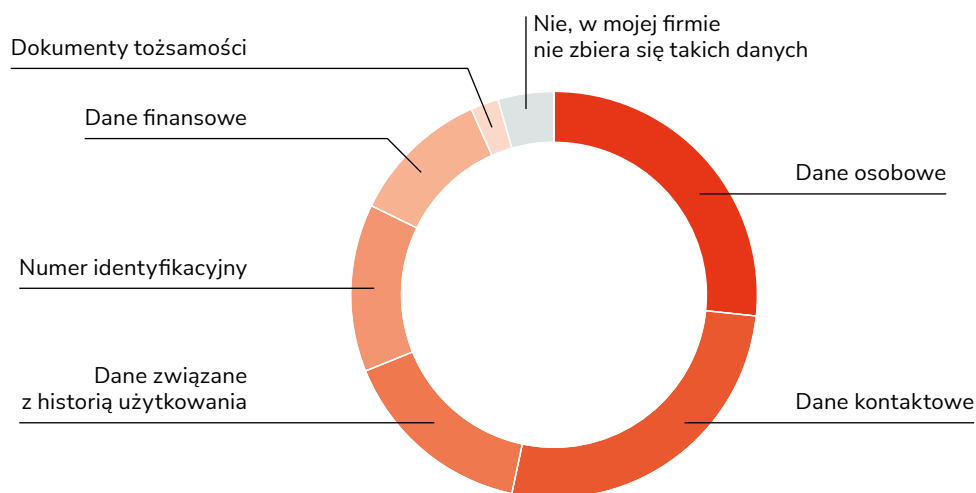
✂ Czy informuje Pan(i) klientów o zagrożeniach w sieci?



Copyright by NASK

Wyniki te wskazują, że firmy stosują różnorodne strategie komunikacyjne, aby edukować swoich klientów w zakresie zagrożeń w sieci. Jednak istnieje potencjał do dalszego rozwoju w obszarze edukacji klientów, zwłaszcza w kontekście dynamicznie zmieniającego się krajobrazu cyberbezpieczeństwa. 13 zbadanych przez nas firm zbiera dane służące do weryfikacji informacji o kliencie, 2 nie zbierają takich informacji. Najczęściej są to dane osobowe i dane kontaktowe, np.: numer telefonu, adres e-mail (po 12 odpowiedzi), dane związane z historią użytkownika, np.: historia zakupów, logowanie się na konto (7), numer identyfikacyjny, np.: PESEL, numer dowodu osobistego lub inny unikalny numer identyfikacyjny wydany przez państwo (6) i dane finansowe, np.: numer konta bankowego, karta kredytowa/debetowa (5). Najrzadziej stosowany jest skan lub zdjęcie dokumentu tożsamości (1), który może służyć w celu bardziej szczegółowej weryfikacji tożsamości klienta, ale jego przetwarzanie było wielokrotnie wskazywane przez UODO jako nadmiarowe. Warto zauważyć, że tylko jedna firma zadeklarowała zbieranie daty urodzenia.

✘ Czy w Pana/Pani firmie zbiera się dane służące do weryfikacji informacji o kliencie?



Copyright by NASK

KOMENTARZ EKSPERTA

W pierwszej kolejności warto docenić fakt przeprowadzenia takiej ankiety przez NASK wśród jego partnerów. Znaczny wzrost skali zagrożeń w obszarze usług cyfrowych oraz zmiany otoczenia regulacyjnego (Akt o Usługach Cyfrowych, NIS2, DORA czy CER i AI ACT), w których środku jesteśmy, są doskonałym momentem na uchwycenie stanu wiedzy i praktyk przedsiębiorców, którzy odpowiadają za tak ważny element gospodarki cyfrowej, jakim jest proces rejestracji i utrzymania domeny internetowej.

W obszarze stosowanych zabezpieczeń wyniki pokazują, że wieloetapowe (ale czy wieloskładnikowe?) uwierzytelnianie, stało się standardem autoryzacji, co należy ocenić bardzo pozytywnie, mając w głowie stan rynku sprzed 3–4 lat. Aktualizacja oprogramowania, stosowanie firewalli, szyfrowanie danych czy nawet monitoring systemów też cieszą i mogą oznaczać, że ankietowani przedsiębiorcy albo certyfikują swoją działalność operacyjną, albo mogliby się do tego przygotować. Wydaje się, że tezę tę wspiera fakt, że 10 na 15 prowadzi analizy

ryzyk dotyczących bezpieczeństwa świadczonych usług cyfrowych. Oczywiście diabeł jak zwykle tkwi w szczegółach i warto byłoby ten wątek pogłębić w kolejnych edycjach badania. Nadchodzące wdrożenie Dyrektywy NIS2 będzie do tego dobrym pretekstem, chociaż jej literalna lektura wydaje się nie obejmować swoim zakresem samej usługi rejestracji domeny internetowej (choćby usługa utrzymania DNS już z pewnością pod NIS2 podpada).

Odpowiedzi na pytanie o „statystyki naruszeń przepisów dot. nielegalnego charakteru treści” pokazuje w mojej opinii, że albo większość respondentów nie świadczy usług w zakresie hostingu (które z punktu widzenia samej usługi rejestracji domeny nie muszą przecież być świadczone), albo nie uznali oni, że takich usług dotyczy ankieta. Warto w tym miejscu zaznaczyć, że dostawcy hostingu (ale nie pośrednicy w rejestracji domen) muszą stosować od początku tego roku europejski Akt o Usługach Cyfrowych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065) wprowadzający znacznie dalej

niż we wcześniejszych latach idącą odpowiedzialność za treści udostępnianie z wykorzystaniem usług hostingu czy platform cyfrowych.

Pozytywnie oceniam także wyniki ankiety w zakresie zbieranych przez dostawców danych służących do weryfikacji informacji o kliencie.

Mariusz Busiło

WSPÓLNIK W KANCELARII BĄCAL BUSIŁO SP. K.,
BĘDĄCEJ CZŁONKIEM POLSKIEJ IZBY INFORMATYKI I TELEKOMUNIKACJI

Wynika z nich w mojej opinii, że większość respondentów ogranicza te dane do minimum niezbędnego do identyfikacji i obsługi biznesowej związanej ze świadczeniem usługi rejestracji domeny. Wyjątkiem są dane, które mogą być uznane za nadmiarowe jak wizerunek czy data urodzenia.

vishing

szyfrowanie

IPS

encryption

software

analysis

ryzyko

oprogramowanie

system

IDs

security

authentication

antivirus

risk

firewall

monitoring

uwierzytelnianie

phishing

spoofing

monitoring

update

aktualizacja



Rynek i promocja on-line

Jak się reklamować w Internecie – przegląd praktyk na wybranych przykładach

Ankieta pokazuje, że 11 z 15 badanych przez nas firm korzysta z jakiejś formy reklamy internetowej lub innych form promocji on-line. Najczęściej są to reklamy w mediach społecznościowych (9 wskazań), reklamy w wyszukiwarkach (SEM) (7), mailowe kampanie marketingowe (6), marketing treści (np.: sponsorowane artykuły, e-booki, filmiki) (5). Rzadziej stosowane są reklamy displayowe (np. banery, pop-up'y) (3), reklamy wideo np.: krótkie spoty reklamowe, filmy instruktażowe czy treści promocyjne, reklamy mobilne, np.: w aplikacjach mobilnych, reklamy interaktywne czy natywne (2) i fora internetowe (1).

✂ Z jakich form reklamy internetowej czy innych form promocji on-line korzysta Pana/Pani firma?



z nich należą cel działalności (nowa firma, nowy projekt itp.) – 12 wskazań, ochrona marki – 11, budowanie marki – 9, dostępność nazwy – 9, SEO (optymalizacja pod wyszukiwarki), strategia długoterminowa – 7, cel zasięgów (regionalnie, globalnie) – 6, personalizacja – 4 oraz trendy – 3. Jedna z firm miała problem z odpowiedzią na to pytanie.

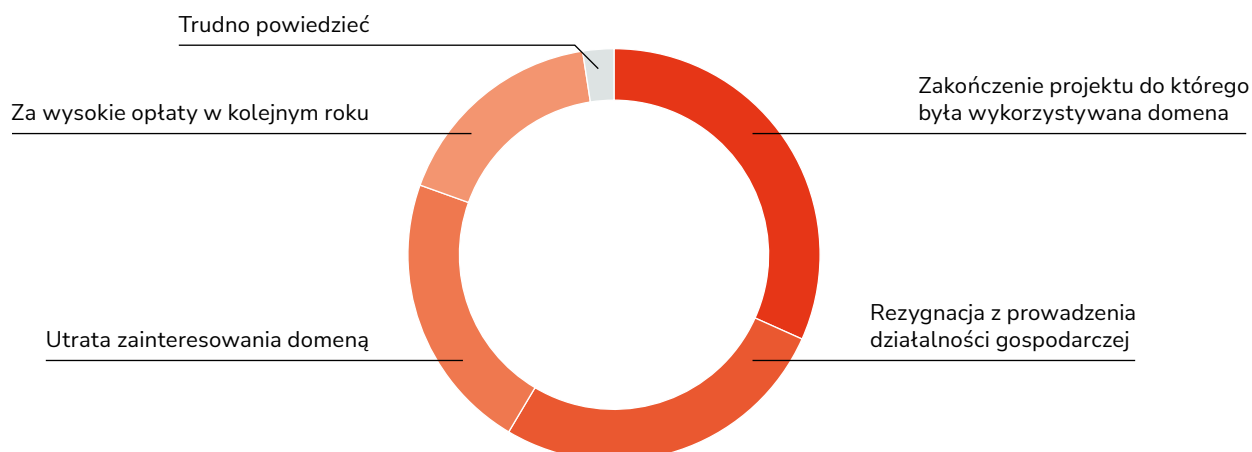
✘ Jakie czynniki najczęściej wpływają na decyzję klientów Pana/Pani firmy o rejestrowaniu nowych domen?



Copyright by NASK

Badane firmy często borykają się z problemem nie odnawiania domen przez swoich klientów. Jako najczęstsze powody wskazują zakończenie projektu do którego była wykorzystywana domena (13), rezygnację z prowadzenia działalności gospodarczej (11), utratę zainteresowania domeną (9), a także za wysokie opłaty w kolejnym roku (7). Jedna z firm miała problem z odpowiedzią na to pytanie.

✘ Jakie według Pani/Pana są główne przyczyny, dla których abonenci decydują się nie odnawiać swoich domen?

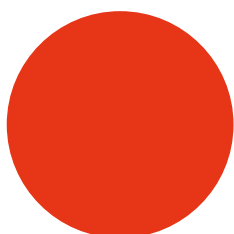


Copyright by NASK

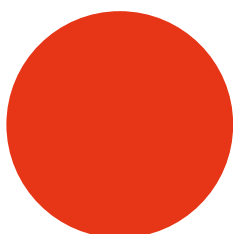
Niektóre z firm, aby zapobiec problemowi nie odnawiania domen, oferują swoim klientom promocje. Robi tak 9 na 15 badanych przez nas firm. Ich częstotliwość nie jest jednak duża. Jedynie 2 firmy robią to kilka razy w miesiącu, 4 kilka razy w roku, a 3 raz w roku lub rzadziej.

Do najczęściej stosowanych przez badane firmy promocji należą rabaty na rejestrację i programy partnerskie (6), promocje na pakiet produktów/usług, pakiety wielu domen, promocje sezonowe lub okolicznościowe, programy lojalnościowe i promocje na dodatkowe usługi (4). Rzadziej stosowane są bezpłatne dodatki (np.: certyfikaty SSL, e-mail, ochrona prywatności danych WHOIS) (3) oraz odnowienia w promocyjnych cenach (2).

✂ Jakie są to promocje?



Rabaty na rejestrację



Programy partnerskie



Promocje na pakiet produktów/usług



Pakiety wielu domen



Promocje sezonowe lub okolicznościowe



Programy lojalnościowe



Promocje na dodatkowe usługi



Bezpłatne dodatki



Odnawienia w promocyjnych cenach

KOMENTARZ EKSPERTA

Powyższe deklaracje wskazują, że rodzime firmy korzystają z zestawu najbardziej efektywnych narzędzi do pozyskiwania tzw. „leadów”, stosowanych na całym świecie przez podmioty skupiające się na sprzedaży B2B. Według raportu publikowanego przez emarketer „The State of the Digital Marketing Channels and Tools” z czerwca 2023 marketerzy z sektora IT zapytani o najbardziej efektywne źródła, tudzież platformy, wskazywali kolejno SEO – 69,7%, marketing treści (content marketing) – 50,6%, social media – 37,8%, marketing rekomendacji (referral marketing) – 30,7% oraz email marketing – 27,0%. Mniejsza liczba wskazań dotyczyła reklamy display (7,5%) oraz video (6,2%). Polska, ekspercka próbka wyrażona w zebranych deklaracjach, w dużej mierze odzwierciedla więc obserwacje gromadzone na całym świecie. Taka hierarchia punktów styku wynika przede wszystkim ze specyfiki

działań marketingowych B2B, w tym relatywnie częstszych (w porównaniu do kampanii konsumenckich) kampanii typowo efektywnościowych, mających generować pożądane interakcje z nowymi i aktualnymi klientami. W przyszłości możemy się spodziewać:

- coraz większej roli tzw. social mediów, wraz z rosnącym udziałem młodszych generacji decydentów wśród klientów usług B2B, wychowanych na mediach społecznościowych, – niezmiennie znacznego zaangażowania działań oraz narzędzi z obszarów SEM oraz SEO, będących efektywnym filarem wielu działań B2B,
- rosnącego znaczenia i zaangażowania środków w marketing treści umożliwiający sprofilowaną i kontekstową komunikację do wybranych, specyficznych odbiorców usług B2B.

Paweł Orkwiszewski

CHIEF STRATEGY OFFICER, IPG MEDIABRANDS

Indeks pojęć

Dotyczący form reklamy internetowej

REKLAMY W MEDIACH SPOŁECZNOŚCIOWYCH – wykorzystują popularność platform takich jak Facebook, Instagram czy LinkedIn, aby dotrzeć do szerokiego grona odbiorców.

REKLAMY W WYSZUKIWARKACH (SEM – SEARCH ENGINE MARKETING) – to ogół działań marketingowych prowadzonych za pomocą wyszukiwarek, na które składają się SEO (Search Engine Optimization) i płatne linki PPC (Pay Per Click). Obydwie wymienione techniki mają wzajemny wpływ na siebie. Bierze się to stąd, iż korzystając z linków sponsorowanych, zwiększamy ruch na stronie, co ostatecznie wpływa również pozytywnie na pozycję w organicznych wynikach wyszukiwania. To szczególnie istotne dla firm, które chcą być widoczne w wynikach wyszukiwania dla konkretnych fraz kluczowych.

MAILOWE KAMPANIE MARKETINGOWE – to forma marketingu bezpośredniego, wykorzystująca pocztę elektroniczną jako narzędzie komunikacji. Jest to najtańsza i najskuteczniejsza metoda dotarcia do obecnych i potencjalnych klientów, której zadaniem jest budowanie i podtrzymywanie relacji i sprzedaży oferowanych usług czy produktów.

MARKETING TREŚCI (CONTENT MARKETING) – to strategia, której istotą jest pozyskanie potencjalnych klientów dzięki publikowaniu atrakcyjnych dla ścisłej grupy odbiorców przekazów. Jako alternatywna forma marketingu ma za zadanie nawiązanie relacji z klientem przez zaangażowanie obu stron (interakcja). Koncepcja tego marketingu oparta jest na tworzeniu i dostarczaniu klientom potrzebnych i użytecznych treści w atrakcyjnych formach (artykuły, poradniki, ebooki, video, podcasty, webinary i inne), a przez to zdobywanie ich zaufania tak bardzo potrzebnego w procesie sprzedaży.

REKLAMY DISPLAYOWE – w postaci graficznego banera reklamowego bądź filmu są formą promocji on-line, która ma na celu przyciągnięcie uwagi użytkowników na stronach internetowych.

REKLAMY WIDEO – takie jak krótkie spoty reklamowe czy filmy instruktażowe, są stosowane przez niektóre firmy, aby przyciągnąć uwagę za pomocą dynamicznych treści wideo.

REKLAMY MOBILNE – w tym reklamy w aplikacjach mobilnych czy natywne reklamy na urządzeniach mobilnych, stają się coraz bardziej popularne ze względu na rosnącą liczbę użytkowników korzystających z urządzeń mobilnych.

Dotyczący czynników wpływających na rejestrację domen

CEL DZIAŁALNOŚCI (NOWA FIRMA, NOWY PROJEKT ITP.) – wybór domeny związany z celem działalności firmy, nową firmą lub projektem jest jednym z kluczowych czynników decydujących dla klientów. Chcą oni, aby domena odzwierciedlała charakter i cele ich działalności.

OCHRONA MARKI – wprowadzanie nowych domen w ramach strategii ochrony marki jest ważne dla klientów, którzy starają się zabezpieczyć swoje unikalne nazwy przed potencjalnymi nadużyciami.

BUDOWANIE MARKI – wybór domeny z myślą o budowaniu marki jest kluczowy dla klientów, którym zależy na skutecznym komunikowaniu swojego wizerunku i przekazu marketingowego.

DOSTĘPNOŚĆ NAZWY – dostępność wybranej nazwy jest istotnym czynnikiem decyzyjnym. Klienci mogą wybierać domeny, które są łatwo dostępne i niekolidują z innymi.

SEO (SEARCH ENGINE OPTIMISATION) – optymalizacja strony www bądź sklepu pod wyszukiwarki – działania mające na celu pozyskanie jak największej liczby odwiedzających Twoją stronę z organicznych wyników Google. Optymalizacja pod kątem wyszukiwarek (SEO) jest ważna dla klientów, którzy chcą zapewnić, że ich domeny będą łatwo znajdowane w wynikach wyszukiwania.

STRATEGIA DŁUGOTERMINOWA – decyzje dotyczące domen często są podejmowane w kontekście długoterminowej strategii biznesowej. Klienci zwracają uwagę na perspektywy rozwoju i ewolucji swojej firmy.

CEL ZASIĘGÓW (REGIONALNIE, GLOBALNIE) – klienci biorą pod uwagę zakres swojej działalności, wybierając domeny, które najlepiej odzwierciedlają ich plany regionalne lub globalne.

PERSONALIZACJA – personalizacja nazwy domeny w celu lepszego dopasowania do specyfiki biznesu lub branży jest istotnym aspektem dla niektórych klientów.

TRENDY – niektórzy klienci decydują się na domeny, które odzwierciedlają aktualne trendy w branży lub społeczeństwie.

Dotyczący form promocji

RABATY NA REJESTRACJĘ – są jednym z najczęściej stosowanych rodzajów promocji. To atrakcyjna oferta dla klientów, którzy chcą skorzystać z obniżonych cen podczas rejestracji nowych domen.

PROGRAMY PARTNERSKIE – pozwalają klientom zdobywać korzyści za polecenie usług firmowych innym potencjalnym klientom. To skuteczny sposób na zwiększenie zasięgu i zdobywanie nowych klientów.

PROMOCJE – obejmujące pakiet produktów lub usług są skierowane do klientów, którzy korzystają z różnych ofert firmy. To zachęta do wybrania kompleksowej gamy usług.

PAKIETY WIELU DOMEN – oferty obejmujące pakiety wielu domen są atrakcyjne dla klientów, którzy potrzebują rejestracji kilku domen naraz. To może obejmować różne rozszerzenia domenowe czy różne nazwy.

PROMOCJE SEZONOWE LUB OKOLICZNOŚCIOWE – są dostosowane do konkretnych okresów, takich jak święta czy dni specjalne. To sposób na przyciągnięcie uwagi klientów w określonych momentach.

PROGRAMY LOJALNOŚCIOWE – nagradzają stałych klientów, poprzez oferowanie im dodatkowych korzyści za długoletnie korzystanie z usług firmy.

PROMOCJE NA DODATKOWE USŁUGI – rabaty na dodatkowe usługi stanowią zachętę dla klientów, którzy chcą skorzystać z różnorodnych funkcji lub opcji dostępnych w ofercie firmy.

BEZPŁATNE DODATKI – (np.: certyfikaty SSL, e-mail, ochrona prywatności danych WHOIS) – oferowanie bezpłatnych dodatków, takich jak certyfikaty SSL, usługi e-mail czy ochrona

Źródła

1. Baran P., *On Distributed Communications Networks*” in: *IEEE Transactions on Communications Systems*, vol. 12, no. 1, pp. 1–9, March 1964, doi: 10.1109/TCOM.1964.1088883.
2. Baran P., *Some changes in information technology affecting marketing in the year 2000*, The Rand Corporation 1968.
3. *Content marketing – koncepcja marketingu alternatywnego na przykładzie firm kurierskich*, „Zeszyty Naukowe Politechniki Śląskiej” 2015, nr kol. 1929, <https://yadda.icm.edu.pl/baztech/element>; dostęp: 05.04.2024.
4. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)*, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2555>.
5. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE*, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022L2557>.
6. Emarketer, *The State of the Digital Marketing Channels and Tools*, 2023.

7. European Union, *European Commission, eGovernment Benchmark 2023 Insight Report. Connecting Digital Governments*, 2023.
8. Fundacja DigitalPoland, *Dezinformacja oczami Polaków*, Warszawa 2024.
9. *Funkcjonalność narzędzi Google w search engine marketingu*, „Studia i prace Wydziału Nauk Ekonomicznych i Zarządzania” nr 39, T. 2; 2015; US; https://wneiz.pl/nauka_wneiz/sip/sip39-2015; dostęp: 05.04.2024.
10. GUS, *Rocznik Statystyki Międzynarodowej*, Warszawa 2023.
11. *Rola e-mail marketingu w komunikacji z interesariuszami szkoły wyższej*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach”, nr 255, 2016, <https://cejsh.icm.edu.pl>; dostęp: 05.04.2024.
12. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)*, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32022R2065>.
13. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011*, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX%3A32022R2554>.
14. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>.
15. Weibel P., *The Post-media Condition*, in: AAVV, *Postmedia Condition*, Centro Cultural Conde Duque, Madrid 2006.

O wydawcy raportu

NASK jest państwowym instytutem badawczym nadzorowanym przez Ministerstwo Cyfryzacji.

NASK-PIB prowadzi obecnie wielowymiarową działalność, operując na styku nauki i biznesu. Do głównych aktywności NASK należy zapewnienie bezpiecznego Internetu i ochrona jego użytkowników. **Cyberbezpieczeństwo i ochrona użytkowników** – Kluczowym polem aktywności NASK są działania związane z zapewnieniem bezpieczeństwa Internetu. Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci w Polsce i koordynacją działań w tym obszarze zajmuje się Pion Centrum Cyberbezpieczeństwa, w którego skład wchodzi m.in. zespół CERT Polska (www.cert.pl). Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK-PIB został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy. NASK współtworzy także zaplecze analityczne oraz badawczo-rozwoje dla krajowego systemu cyberbezpieczeństwa.

Nauka i innowacje – NASK prowadzi działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych (<https://science.nask.pl/>). Tym, co wyróżnia nasz instytut badawczy od ściśle komercyjnych przedsiębiorstw jest podejście do tworzenia rozwiązań dla obecnych i przyszłych potrzeb klientów. W instytucie NASK badacze komercyjny problem ujmują w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, ale również innowacyjnych. Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie, analiza, przetwarzanie i transfer danych, a także złożone systemy sieciowe, w tym systemy IoT oraz mobilne sieci ad hoc. Istotne miejsce zajmują badania dotyczące biometrycznych metod weryfikacji tożsamości w bezpieczeństwie usług. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki. NASK prowadzi także rejestr nazw w domenie .pl (www.dns.pl).

Ważnym elementem działalności NASK jest też edukacja użytkowników oraz promowanie koncepcji społeczeństwa informacyjnego, głównie w celu ochrony dzieci i młodzieży przed zagrożeniami, związanymi z użytkowaniem nowych technologii. Instytut realizuje projekty kluczowe dla cyfrowej transformacji kraju – Ogólnopolska Sieć Edukacyjna (OSE) oraz Elektroniczne Zarządzanie Dokumentacją (EZD RP).

NASK

Redakcja czasopisma

REDAKTORZY NACZELNI

dr hab. Katarzyna Chałubińska-Jentkiewicz

dr hab. Urszula Soler

SEKRETARZE REDAKCJI

dr Monika Nowikowska

Krystyna Cieniewska

kontakt@journaldot.pl

REDAKCJA RAPORTU

Alina Wiśniewska-Skura

Agata Leszczyńska

Anna Gniadek

Katarzyna Nitychoruk

Jarosław Olchawski

Marzena Pastuszka

KOMUNIKACJA I MARKETING

Monika Balcerzak

monika.balcerzak@nask.pl

tel. +48 885 490 405

NASK