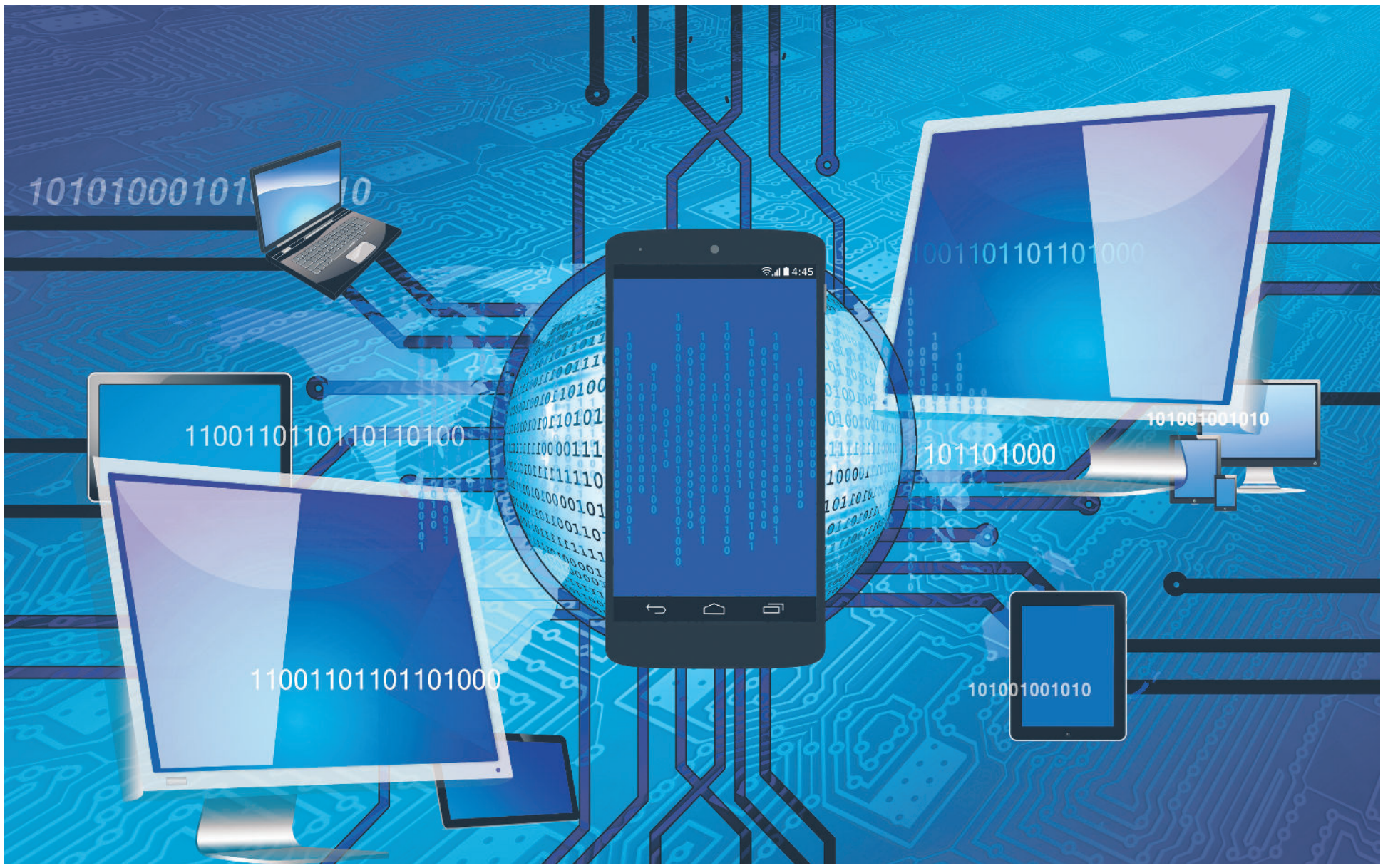
GAZETA FINANSOWA
20–26 września 2019 r.

RYNEK HOSTINGU W POLSCE



Co to jest hosting?

Hosting, usługa hostingowa (hosting service) polega na udostępnianiu wydzielonej przestrzeni dysku twardego serwera wraz z pakietem usług (oprogramowaniem) decydującym o możliwości zagospodarowania tej przestrzeni i komforcie korzystania z niej.

dr Karol **Król**

pracownik naukowo-dydaktyczny Wydziału Inżynierii Środowiska i Geodezji Uniwersytetu Rolniczego w Krakowie. Główny redaktor serwisu digitalheritage.pl.

Hostować znaczy utrzymywać, gościć, a od strony technicznej – wydzierżawiać przestrzeń dysku twardego serwera. Na usługę hostingową składa się zatem infrastruktura (sprzęt, hardware) oraz oprogramowanie (software). Jak w przypadku każdej usługi, również w kontekście usług hostingowych można wyróżnić parametry decydujące o ich jakości i atrakcyjności.

Usługi w pakiecie hostingowym

Do podstawowych usług dostępnych w pakiecie hostingowym zaliczyć można konta FTP i towarzyszącego im klienta FTP (menedżera plików) do ich obsługi w oknie przeglądarki internetowej. Usługa FTP (File Transfer Protocol) służy do przesyłania plików za pośrednictwem sieci. Konfiguracja połączenia FTP pozwala na bezpośrednie połączenie się z dyskiem serwera. W ramach zarządzania usługą FTP możliwe jest wyodrębnienie fragmentu dzierżawionej przestrzeni i udostępnienie jej innym użytkownikom. Konfiguracja i nawiązanie połączenia umożliwia przesyłanie plików z dysku lokalnie na serwer danych.

Do podstawowych usług w pakiecie hostingowym zaliczyć można także bazy danych MySQL. Baza danych MySQL umożliwia uruchamiane aplikacji bazodanowych takich jak np. systemy zarządzania treścią CMS. Dostęp do bazy danych warunkowany jest znajomością: hosta, nazwy użytkownika, hasła dostępu oraz nazwy bazy danych. Obecnie instalacja większości systemów CMS możliwa jest bezpośrednio z panelu zarządzania usługa hostingową. W większości przypadków wraz z instalacją automatycznie tworzona jest baza danych niezbędna do uruchomienia CMS. Znacząco skraca to czas instalacji CMS.

Zarządzanie domeną internetową

Oprogramowanie pakietu hostingowego pozwala zarządzać domenami, w tym dopisywać i parkować domeny, tworzyć subdomeny i przekierowania. Pakiet hostingowy pozwala także zarządzać kontami e-mail i ustawieniami poczty elektronicznej. W przypadku większości usług możliwa jest ich obsługa (konfiguracja) na poziomie podstawowym, jak i zaawansowanym. Przydatna bywa także usługa CRONE, która umożliwia cykliczne wywoływanie określonych zadań.

Hosting płatny czy bezpłatny?

Według raportu Global Web Hosting Market Share, wartość polskiego rynku usług hostingowych w 2016 roku wyniosła niemal 406 mln USD. Dało to Polsce 13. miejsce pod względem udziału w rynku światowym z wynikiem 1,3 proc. i 8 miejsce w Europie[1]. Przewiduje się, ze ważnym czynnikiem powodującym wzrost rynku hostingowego w Polsce będzie przenoszenie usług do chmury (cloud computing) w celu zwiększania elastyczności biznesowej i ograniczania kosztów związanych z ICT[2].

Alternatywą dla usług hostingowych świadczonych komercyjnie są te udostępniane bezpłatnie. Do najbardziej znanych dostawców darmowych usług hostingowych w Polsce należą hostinger.pl, cba.pl, prv.pl, friko.pl. Zakres i jakość bezpłatnych usług hostingowych bywa różna. Prognozuje się, że znaczenie bezpłatnego hostingu będzie maleć z uwagi na spadek cen usług komercyjnych oraz ich zakres i jakość. Wady bezpłatnych usług hostingowych wyszczególnili Król i Zdonek[2].

Darmowy hosting jest często traktowany przez usługodawców jako swoisty „koszt pozyskania nowego klienta", który owszem ma do dyspozycji usługę darmową, jednak jest ona ściśle limitowana, a sam użytkownik jest regularnie zachęcany do skorzystania z pakietu płatnego.

Dostawcy bezpłatnych usług hostingowych najczęściej nie dają żadnych gwarancji jakości (niezawodności). Znajduje to odzwierciedlenie w regulaminach usług. Ponadto najczęściej brak tu jakiegokolwiek wsparcia technicznego. Awarie techniczne mogą się wiązać z bezpowrotną utratą danych bez możliwości wniesienia reklamacji.

Brak niezawodności usług oraz dostępu do infolinii i bezpośredniej pomocy technicznej właściwie dyskwalifikuje bezpłatne usługi hostingowe jako podstawę infrastruktury dla witryn biznesowych. W ocenie Króla i Zdonka[2] bezpłatne usługi hostingowe mogą znaleźć zastosowanie jako swoisty „poligon doświadczalny" w projektach amatorskich i szkoleniowych.

Źródła

1. Serwis ISBNews, Raport: Biznes Wartość polskiego rynku usług hostingowych sięga niemal 406 mln USD z dnia 24.11.2016 r. stooq.pl

2. Król, K., Zdonek, D. (2017). Charakterystyka rynku usług hostingowych w Polsce. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 102, 157-167. DOI: http://dx.doi.org/10.29 119/1641-3466.2 017 102.13

GLOBALNY LIDER TECHNOLOGICZNY: NAZWA.PL

Rozmowa z Krzysztofem Cebratem, prezesem zarządu spółki nazwa.pl

Jak rozwija się polski rynek rejestracji domen i hostingu?

W Polsce mamy obecnie 2,6 miliona nazw zarejestrowanych w rozszerzeniu .pl. Ich liczba jest na poziomie zbliżonym do tego sprzed pięciu lat, a dynamiczny rozwój tego rynku jest już za nami. Charakterystyczne dla rynku dojrzałego, z jakim mamy obecnie do czynienia, jest to, że nie pojawiają się już nowe podmioty świadczące usługi hostingowe. Z kolei firmy, których udział w rynku nie przekracza kilku procent, poprzez konsolidację, są wchłaniane przez większe spółki prawa handlowego. To naturalny proces, który obserwowaliśmy także w innych sektorach polskiej gospodarki.

Obecna sytuacja stawia przed uczestnikami rynku nowe wyzwania, które są podyktowane rosnącą świadomością klientów i ich oczekiwaniami.

Rynek w Polsce będzie rozwijał się w kierunku dostarczania kompleksowych, bardziej zaawansowanych technologicznie rozwiązań, które mają na celu zwiększać bezpieczeństwo klientów. To będzie ze sobą niosło konieczność dokonywania znaczących nakładów inwestycyjnych, na rozwój technologii i implementacje rozwiązań, na które stać będzie tylko nielicznych. Kto spełni oczekiwania klientów, ten będzie, na tym dojrzałym rynku, miał najwięcej do powiedzenia.

Na co zwrócić uwagę przy rejestracji domeny internetowej?

Współczesna sieć pełna jest zagrożeń, dlatego warto wybrać Rejestratora, który nie tylko dokona rejestracji wymarzonej nazwy, ale również zadba o nasze bezpieczeństwo. Na polskim rynku większość firm oferuje jedynie rejestrację domeny internetowej. To zdecydowanie za mało! W wyniku rejestracji domeny powstaje wpis, który informuje, które serwery DNS w sieci Internet odpowiadają za obsługę naszej nazwy oraz, co najważniejsze dla bezpieczeństwa, czy domena zostaje lub nie zostaje zabezpieczona **za pomocą DNSSEC**. Zabezpieczenie to uniemożliwia podszywanie się pod naszą domenę, a tym samym stronę WWW i konta poczty elektronicznej. Oprócz stosowania zabezpieczenia DNSSEC, warto zwrócić uwagę czy Rejestrator świadczy w jej ramach usługę DNS w **technologii Anycast**. To właśnie ta technologia serwerów DNS chroni Klientów nazwa.pl przed atakami DDoS oraz zapewnia **błyskawiczne ładowanie ich serwisów WWW** z dowolnego miejsca na Ziemi. Kolejnym zabezpieczeniem, będącym standardem w nazwa.pl, jest DNS over TLS. To unikalna w Polsce usługa oferowana przez nazwa.pl w ramach usługi rejestracji domeny. Zabezpiecza za pomocą szyfrowanych połączeń SSL całą transmisję do serwerów DNS Anycast nazwa.pl. Skoro nikt nie chce, aby jego połączenia do stron WWW lub poczty e-mail były podsłuchiwane, to czemu miałby pozwalać, aby ktoś „podsłuchiwał" z jakimi adresami w sieci Internet się łączy? Powinniśmy powierzać rejestrację domen tylko tym Firmom, które mają własne akredytacje i nie korzystają z pośredników, którym przekazują dane osobowe klientów. Dla nazwa.pl to standard. **Nazwa.pl to jedyna polska firma, która może świadczyć usługi rejestracji domen globalnych bez pośredników, zapewniając bezpieczeństwo zarejestrowanych domen na mocy prawa polskiego!**

Taka właśnie kompleksowa i rozbudowana usługa Bezpieczna Domena wzbudza zaufanie klientów. To zaufanie ma wymierne skutki, nazwa.pl będąc liderem rynku, obsługuje co czwartą domenę w Polsce. W styczniu 2019 roku spółka została uznana przez Ministerstwo Cyfryzacji **za operatora usługi kluczowej** w sektorze infrastruktury, polegającej na prowadzeniu autorytatywnego serwera DNS. Wpisanie nazwa.pl na listę operatorów usług kluczowych dla cyberbezpieczeństwa Polski, niesie dla spółki konieczność utrzymywania najwyższych środków technicznych i organizacyjnych, dla klientów z kolei oznacza realizację najwyższych światowych standardów, niedostępnych w innych polskich firmach hostingowych. Koszty nakładów inwestycyjnych to miliony złotych. Bezpieczeństwo klienta nie powinno być jednak poddawane kompromisom.

Spółka nazwa.pl od lat jest liderem nie tylko, jeśli chodzi o rejestrowane domeny, ale również o usługi hostingowe. Czym kierują się klienci wybierając właśnie wasze usługi?

Wybór domeny oraz hostingu to bardzo ważna decyzja dla każdego przedsiębiorcy. Szybkość, stabilność oraz bezpieczeństwo usług i danych naszych Klientów to podstawowe kryteria, jakimi powinniśmy kierować się przy wyborze usług.

Badania przeprowadzone przez Google wskazują, że prawdopodobieństwo opuszczenia mobilnej strony wzrasta o 32 proc., jeżeli czas jej ładowania przekroczy 3 sekundy. Kto prowadząc biznes może sobie pozwolić na takie straty? Aby przyspieszyć działanie stron WWW firma nazwa.pl uruchomiła sieć serwerów DNS Anycast na wszystkich zamieszkałych kontynentach, od USA po Japonię i Australię.

Spółka jest jedynym dużym dostawcą w Polsce, który usługi hostingowe świadczy w oparciu o chmurę obliczeniową. Technologia ta zapewnia skalowalność, pozwalającą na obsługę nawet bardzo dużego ruchu na stronie WWW, gdyż wzmożona ilość zapytań jest rozkładana na wiele fizycznych serwerów. Takie rozwiązanie pozwala obsłużyć bardzo dużą liczbę zapytań jednocześnie, bez wpływu na działanie serwisu WWW, a co za tym idzie – dynamicznie rozwijać biznes w Internecie.

Firma nazwa.pl korzysta z najnowocześniejszej infrastruktury światłowodowej o łącznej przepustowości z siecią Internet ponad 150 Gbps, zapewniając bezpośredni dostęp Klientom spółki do krajowych i międzynarodowych punktów wymiany ruchu internetowego IX – Internet eXchange. Dzięki strategicznym w skali globalnej punktom wymiany danych Klienci nazwa.pl mają dostęp do bezpośredniej wymiany ruchu z największymi światowymi markami takimi jak: Google, Microsoft, Amazon, Facebook, YouTube czy Instagram. Wydatki poniesione na rozwój infrastruktury to miliony złotych, ale naszym zdaniem to dobra inwestycja, która niesie za sobą szybkość i niezawodność świadczonych dla nich usług.

Dlaczego hosting w chmurze jest tak istotny? Klienci naprawdę przywiązują do tego tak dużą wagę?

Każdy komputer czy też serwer ma ograniczoną moc obliczeniową procesora, ograniczone zasoby dyskowe oraz limitowaną ilość pamięci. W efekcie na tradycyjnym hostingu można zaobserwować okresowe przeciążenia serwera skutkujące spowolnieniem działania stron WWW lub całkowitą ich niedostępnością. Awaria serwera może wystąpić w godzinach najwyższego szczytu, gdy ilość odwiedzających strony WWW jest największa. Tradycyjny hosting podczas awarii uniemożliwia dostęp do strony czy poczty elektronicznej. Usługi po prostu wtedy nie działają.

Tylko chmura może zapewnić skalowalność i niezawodność działania, ponieważ pula zasobów nie jest limitowana do wydajności pojedynczego serwera, a awaria jakiegokolwiek serwera nie powoduje przerwy w działaniu usług. Hosting Cloud to odpowiedź na potrzeby klientów związane z szybkością jak i stabilnością oraz bezpieczeństwem. Takie rozwiązanie pozwala obsłużyć również wzrastający ruch na stronie, wywołany na przykład prowadzoną kampanią reklamową, bez wpływu na szybkość działania serwisu WWW. Co więcej, moc obliczeniowa całego klastra serwerów obsługiwanych przy pomocy takiego rozwiązania może zostać łatwo zwiększana, poprzez dołączanie dowolnej liczby nowych serwerów. Zastosowanie technologii cloud hostingu oznaczało wielomilionowe inwestycje dla spółki. To rozwiązanie przekłada się jednak na najwyższy komfort pracy po stronie klienta, a na tym liderowi technologicznemu, którym jest nazwa.pl, zależy najbardziej.

Dlaczego więc nie każdy dostawca stosuje rozwiązania chmurowe?

Podstawową barierą jest zbyt mała skala prowadzonej działalności oraz bardzo duże początkowe nakłady inwestycyjne, sięgające wielu milionów złotych. To skutecznie wyłącza małe firmy hostingowe z oferowania bezpiecznego i niezawodnego hostingu. Bez względu na ilość obsługiwanych usług hostingowych konieczne jest zbudowanie całej infrastruktury chmury obliczeniowej. Dostawca musi zastosować zwielokrotnioną ilość macierzy dyskowych na wypadek awarii, konieczne jest także wykupienie drogich licencji na oprogramowanie do obsługi chmury obliczeniowej i systemów CRM komunikujących się z chmurą obliczeniową. Klasyczny hosting posiada niski próg wejścia i wymaga jedynie wykupienia usługi dzierżawy serwera fizycznego za kilkaset złotych miesięcznie i licencji na oprogramowanie cPanel/WHMCS. Tradycyjny hosting to technologia, która ma sporo ograniczeń i w obliczu nieustannie rosnącego ruchu w Internecie, coraz bardziej wymagających aplikacji webowych oraz potrzeb związanych z bezpieczeństwem można powiedzieć, że odchodzi do lamusa. Niestety wielu, zwłaszcza małych dostawców kurczowo trzyma się tych rozwiązań, uważając je za wystarczające. Czas tych firm hostingowych dobiega jednak końca, gdyż świadomość i oczekiwania klientów idą w stronę rozwiązań chmurowych. Przyszłość na tym rynku należy do dużych dostawców, których przy odpowiedniej skali biznesu, stać na kosztowne inwestycje.

Czym różnią się oferty hostingu u dostawców tej usługi w Polsce i jak zmieniają się na przestrzeni lat?

Podobnie jak w przypadku rejestracji domeny u różnych Rejestratorów, także w ofercie hostingu w Polsce mamy olbrzymie dysproporcje pomiędzy dostawcami. Kluczowe dla użytkownika są dzisiaj: bezpieczeństwo, szybkość i niezawodność.

Żeby osiągnąć najwyższy, światowy poziom w każdym z tych obszarów konieczne są działania związane z rozwojem infrastruktury i zabezpieczeń, a zatem nakłady rzędu nawet kilkudziesięciu milionów złotych. Na takie wydatki stać tylko nielicznych. Nie dziwi zatem fakt, że tylko klienci największych dostawców mogą liczyć na możliwość korzystania z najnowocześniejszych i najbezpieczniejszych rozwiązań technologicznych. Moim zdaniem na dużych firmach ciąży odpowiedzialność za zwiększanie bezpieczeństwa w sieci. Spółka nazwa.pl tak właśnie pojmuje rolę lidera technologicznego i stale podnosi jakość świadczonych usług. W tym miejscu wspomnę tylko wdrożenia zabezpieczeń na przestrzeni ostatnich dwóch lat: DNSSEC, DNS over TLS, rekord CAA, SPF, DKIM, DMARC, szyfrowanie ECDSA w Certyfikatach SSL.

Spółka uruchomiła **scrubbing center**, czyli specjalistyczną infrastrukturę sprzętowo-programową, której zadaniem jest analiza ruchu IP z sieci Internet, w celu wykrycia oraz odfiltrowania szkodliwego ruchu zagrażającego poprawnemu działaniu serwisów WWW, poczty elektronicznej, DNS i innych usług. Ochrona obejmuje w szczególności eliminację zagrożeń związanych z atakami typu: DDoS, atakami wolumetrycznymi (wysycenie łącza), SYN flood, UDP ICMP flood i DNS lub NTP reflection.

Praktyka rynkowa pokazuje, że pozostałe firmy, konkurujące z nazwa.pl, wdrażają rozwiązania z mniej więcej dwuletnim opóźnieniem w stosunku do lidera. Tak było w przypadku: dysków SSD NVMe, tak dzieje się w przypadku serwerów DNS Anycast, może i tak będzie w przypadku protokołu DNSSEC.

Rozwój biznesu w Internecie, to zarówno szybkość, jak i bezpieczeństwo. Według danych podawanych przez NASK, udział nazwa.pl w liczbie domen polskich, zabezpieczonych przed atakami cyberprzestępców za pomocą protokołu DNSSEC, przekracza 90 proc. Badania własne firmy wskazują równocześnie, że nazwa.pl obsługuje ponad 50 proc. stron z obsługą SSL w Polsce i ponad 95 proc. w zakresie TLS 1.3. Gdyby do tego dodać, że serwery DNS Anycast nazwa.pl jako jedyne w Polsce obsługują DNS over TLS zabezpieczające transmisję do systemu DNS przed podsłuchiwaniem transmisji, to można uznać, że nazwa.pl w zakresie świadczonych usług nie ma już z kim konkurować na rynku polskim. Firma stała się globalnym liderem technologicznym, **a jej usługi są porównywane z usługami światowych liderów takich jak OVH, Cloudflare i Godaddy.**

To oznacza, że Klienci nazwa.pl mogą jako pierwsi w Polsce korzystać z nowych technologii, niedostępnych w ofertach firm konkurencyjnych.

RYNEK HOSTINGU W POLSCE

EGZEKUCJA Z PRAW MAJĄTKOWYCH DO DOMENY INTERNETOWEJ

W świecie rozwoju nowych technologii skuteczne zaspokojenie należności wierzycieli coraz częściej staje się możliwe w wyniku przeprowadzenia egzekucji z praw majątkowych do domeny internetowej. Prawa te w wielu wypadkach posiadają znaczną wartość i stanowią istotny składnik majątku dłużników.

Paweł **Milewski**

adwokat z kancelarii Gardocki i Partnerzy Adwokaci i Radcowie Prawni

Podmiot, który zarejestrował domenę internetową, nie nabywa prawa własności, a jedynie prawo do jej używania w sieci[1]. Wywołuje to taki skutek, że podmiot ten uzyskuje na zasadach wyłączności prawo do posługiwania się nową, zarejestrowaną domeną w sieci. Może on przenieść prawa z domeny internetowej na inny podmiot, może też wydzierżawić domenę i czerpać z tego tytułu pożytki. Prawa do domeny internetowej są bowiem zbywalnymi prawami majątkowymi, a egzekucja z tych praw uregulowana jest w przepisach Kodeksu postępowania cywilnego.

Zaspokoić wierzyciela

Prawo do domeny internetowej zostaje zajęte z chwilą doręczenia zawiadomienia dłużnikowi zajętej wierzytelności. Komornik sądowy w toku egzekucji wysyła zawiadomienie o zajęciu prawa do domeny internetowej do rejestratora domeny, czyli do NASK, ale również do podmiotu pośredniczącego w rejestracji domeny, czyli dla przykładu do home.pl. Z mocy zajęcia wierzyciel może wykonywać wszelkie uprawnienia majątkowe dłużnika wynikające z zajętego prawa, które są niezbędne do zaspokojenia wierzyciela w drodze egzekucji, może również podejmować wszelkie działania, które są niezbędne do zachowania prawa. Działaniami takimi są najczęściej czynności faktyczne i prawne mające na celu zapobieżenie utraty prawa lub doprowadzenia do pomniejszenia jego wartości, np. uiszczenie przez wierzyciela opłaty abonenckiej w celu utrzymania prawa do domeny internetowej.

Rekomendowany sposób egzekucji

Do oszacowania zajętego prawa komornik sądowy powołuje biegłego sądowego. Dodatkowo na wniosek dłużnika i za zgodą wierzyciela możliwa jest sprzedaż prawa do domeny internetowej z wolnej ręki bez oszacowania prawa przez biegłego sądowego. Do zaspokojenia wierzyciela z zajętego prawa dochodzi w wyniku uzyskania dochodów, jakie prawo to przynosi, z realizacji tego prawa lub z jego sprzedaży. Niestety przepisy prawa obowiązujące komorników sądowych w Polsce dotyczące jurysdykcji krajowej uniemożliwiają zajmowanie praw majątkowych z domen ogólnoświatowych. Kancelaria Gardocki i Partnerzy bardzo często w postępowaniach egzekucyjnych rekomenduje wierzycielom korzystanie z tego sposobu egzekucji. Jego zastosowanie coraz częściej przyczynia się do zaspokojenia wierzyciela w ramach prowadzonego postępowania egzekucyjnego.

1 Wyrok Sądu Apelacyjnego w Katowicach z dnia 13-06-2006 r. sygn. akt I ACa 272/06. Rejestracja i utrzymanie domeny w sieci jest świadczeniem odpłatnym, a opłaty ponosi podmiot zarejestrowany w wysokości i za okresy przewidziane w umowie.

Najczęściej atakowani z własnego terytorium

Jak wynika z najnowszej analizy zagrożeń przeprowadzonej przez F5 Labs[1], Europa jest celem większej liczby ataków przeprowadzanych z jej własnego terenu niż jakikolwiek inny region świata. Większość ataków jest inicjowana z adresów IP zlokalizowanych w Holandii, a w dalszej kolejności z tych znajdujących się w Stanach Zjednoczonych, Chinach, Rosji i Francji.

Sara **Boddy**

dyrektor ds. badania zagrożeń, F5 Labs

Europejskie systemy są atakowane z adresów IP z całego świata. Krajem, z którego pochodziło najwięcej ataków, okazała się Holandia. Na kolejnych miejscach pierwszej dziesiątki znalazły się: Stany Zjednoczone, Chiny, Rosja, Francja, Iran, Wietnam, Kanada, Indie i Indonezja. Warto zauważyć, że z Holandii pochodziło 1,5-krotnie więcej ataków na systemy europejskie niż ze Stanów Zjednoczonych i Chin łącznie, a także 6-krotnie więcej niż z Indonezji.

Najczęściej wykorzystywane w atakach sieci (ASN) i dostawcy usług internetowych

Trzy sieci, z których wykryto najwięcej ataków (holenderska sieć HostPalace Web Solutions, francuska – Online SAS i NForce Entertainement z Holandii) to dostawcy usług hostingowych, którzy regularnie pojawiają się na sporządzanych przez F5 Labs listach sieci najczęściej używanych przez cyberprzestępców[2]. 72 proc. wszystkich zarejestrowanych w raporcie numerów ASN[3] reprezentuje dostawców usług internetowych, pozostałe 28 proc. to dostawcy usług hostingowych. W ramach przeprowadzonych badań analitycy F5 Labs wskazali też 50 adresów IP, które są najczęściej wykorzystywane do atakowania celów w Europie[4]. Z tą listą powinni zapoznać się przedsiębiorcy i sprawdzić dzienniki swoich sieci pod kątem połączeń z wyszczególnionymi w niej adresami IP. Ze względów bezpieczeństwa adresom tym powinni się również przyjrzeć właściciele sieci.

Najczęściej atakowane porty

Dzięki analizie najczęściej atakowanych portów, ekspertom z F5 Labs udało się określić typ systemów, które znajdują się na celowniku cyberprzestępców. Najczęściej atakowany port w Europie (port 5060) wykorzystywany jest w telefonii internetowej do komunikacji za pośrednictwem telefonów i systemów wideokonferencyjnych. Jak wynika z analiz ruchu związanego z atakami ukierunkowanymi na określoną lokalizację, port ten regularnie jest celem intensywnych ataków w trakcie globalnych konferencji dyplomatycznych, takich jak niedawne ważne szczyty Donalda Trumpa z Kim Dzong Unem[5] i Władimirem Putinem[6].

Skuteczne zabezpieczenie

Według ekspertów F5 firmy powinny nieustannie skanować swoje systemy i porty pod kątem zewnętrznych luk w zabezpieczeniach, a każdy system narażony na zewnętrzne ataki na porty najczęściej wybierane przez przestępców powinien być traktowany priorytetowo przy konfiguracji zapory lub zarządzaniu lukami w zabezpieczeniach. Administratorzy sieci i inżynierowie zabezpieczeń powinni przejrzeć dzienniki sieci pod kątem połączeń z adresami IP, z których najczęściej pochodzą ataki. W przypadku ich wykrycia należy zgłosić nadużycie właścicielom sieci o danym numerze ASN i dostawcom usług internetowych, aby mogli oni wyłączyć systemy przestępców. Kłopotliwe może być prowadzenie dużych czarnych list, podobnie jak blokowanie adresów IP, które należą do puli adresów określonego dostawcy usług internetowych. Mogą one bowiem zapewniać dostęp do Internetu w miejscach zamieszkania klientów atakowanej firmy. „W takich przypadkach systemem atakującym najprawdopodobniej jest zainfekowane urządzenie IoT, którego właściciele nie zdają sobie sprawy z zagrożenia i nie mają możliwości jego usunięcia. Zablokowanie ruchu z całej sieci o konkretnym numerze ASN lub od określonego dostawcy usług internetowych mogłoby uniemożliwić współpracę użytkowników z daną firmą. W takim przypadku lepszym rozwiązaniem będzie zablokowanie wyłącznie dostawcy usług internetowych obsługującego kraj, z którym dane przedsiębiorstwo nie współpracuje w oparciu o geolokalizację na poziomie kraju.

1 Analitycy F5 Labs we współpracy z firmą Baffin Bay Networks zajmującą się analizą zagrożeń podjęli się zbadania globalnego środowiska ataków, aby lepiej zrozumieć zagrożenia w poszczególnych regionach, wyodrębnić wspólne cechy przestępców i powtarzające się atakowane porty oraz wskazać elementy unikalne. W serii przeprowadzonych badań przeanalizowano ataki, które miały miejsce w tym samym 90-dniowym okresie w Europie, Stanach Zjednoczonych, Kanadzie i Australii. Wnioski z badania F5 Labs zostały wyciągnięte na podstawie analizy ruchu związanego z atakami ukierunkowanymi na europejskie adresy IP w okresie od 1 grudnia 2018 r. do 1 marca 2019 r.

2 https://www.f5.com/labs/search._hunt_for_IoT

3 Autonomous System – zbiór adresów IP pod wspólną administracyjną kontrolą, ze spójną routing policy

4 https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives-europe

5 https://www.f5.com/labs/articles/threat-intelligence/russian-attacks-against-singapore-spike-during-trump-kim-summit

6 https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting

Nowe prawo dla hosting providerów

Unijny ustawodawca zdecydował się zwiększyć ochronę prawną podmiotów uprawnionych z praw autorskich w zakresie związanym z udostępnianiem treści chronionych przez serwisy internetowe. W dniu 17 kwietnia 2019 roku uchwalona została dyrektywa nr 2019/790 w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (przez jej krytyków zwana niekiedy ACTA 2). Państwa członkowskie mają czas na implementowanie przedmiotowej dyrektywy do dnia 7 czerwca 2021 roku.

Robert **Nogacki**

radca prawny,
Kancelaria Prawna Skarbiec

Jak wyjaśnia dyrektywa w punkcie 61 preambuły, w ostatnich latach funkcjonowanie rynku treści online stało się bardziej złożone. Z jednej strony usługi internetowe zapewniają szerszy dostęp do dzieł kultury i nauki, oferując twórcom duże możliwości rozwijania nowych modeli biznesowych, z drugiej strony powstaje pole do nadużyć w zakresie korzystania z treści chronionych bez zezwolenia podmiotów uprawnionych.

Dostawcy usług udostępniania treści online

Remedium na powyższą sytuację ma być regulacja w zakresie korzystania przez dostawców usług udostępniania treści online z treści chronionych. Dyrektywa wprowadza pojęcie dostawcy usług udostępniania treści online, definiując go jako dostawcę usług społeczeństwa informacyjnego, którego głównym lub jednym z głównych celów jest przechowywanie i udzielanie publicznego dostępu do dużej liczby chronionych prawem autorskim utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników tych usług, które są przez niego organizowane i promowane w celach zarobkowych. Spod powyższego pojęcia wyłączono dostawców takich usług, jak nienastawione na zysk encyklopedie internetowe, nienastawione na zysk repozytoria naukowe i edukacyjne, platformy tworzenia otwartego oprogramowania i platformy wymiany otwartego oprogramowania, dostawców usług łączności elektronicznej zdefiniowanych w dyrektywie (UE) 2018/1972, internetowych platform handlowych oraz usług w chmurze dla przedsiębiorstw i usług w chmurze obliczeniowej, które umożliwiają użytkownikom zamieszczanie treści na własny użytek.

Zgoda twórcy

Regulacja art. 17 omawianej dyrektywy wprowadza wymóg uzyskiwania przez dostawcę usług udostępniania sieci online stosownego zezwolenia od podmiotu uprawnionego w sytuacji w której użytkownik serwisu internetowego zamieszcza w nim treści objęte ochroną prawnoautorską, co do których nie ma uprawnień. Innymi słowy jeśli w ramach danego portalu użytkownicy zamieszczają treści chronione prawem autorskim, to właściciel tego portalu powinien zadbać o to, aby uzyskać zezwolenie od podmiotu uprawnionego. Jeśli bowiem dostawca usług udostępniania sieci online udziela publicznego dostępu do treści zamieszanych przez użytkowników serwisu, które są chronione prawem autorskim, to dyrektywa nakazuje traktować takie działanie jako dokonywanie przez przedmiotowego dostawcę czynności publicznego udostępniania lub czynności podawania do publicznej wiadomości. Zatem, aby pozostawać w zgodzie z prawem, właściciel serwisu powinien na przykład zawrzeć stosowną umowę licencyjną w celu publicznego udostępnienia lub podania do publicznej wiadomości utworów (które w jego serwisie zamieszczają użytkownicy). Obowiązek ten stanowi istotne novum w unijnych regulacjach z zakresu dziedziny prawa autorskiego.

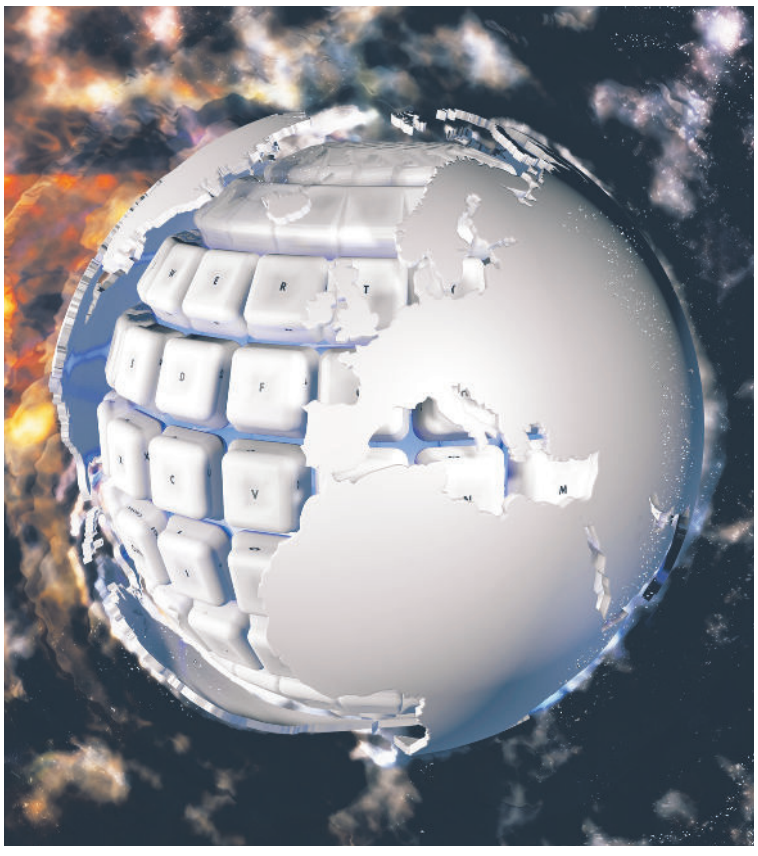
Nowe zasady odpowiedzialności

Dotychczas zasady odpowiedzialności hosting providera określał art. 14 dyrektywy 2000/31/WE o handlu elektronicznym, który został implementowany w art. 14 polskiej ustawy o świadczeniu usług drogą elektroniczną. Co do zasady zawiera on wyłączenie odpowiedzialności właściciela serwisu za treści umieszczane przez użytkowników, jeśli zarazem zostały spełnione określone warunki (m.in. brak wiedzy o bezprawnym charakterze danych oraz niezwłoczne ich usunięcie po otrzymaniu urzędowego zawiadomienia lub po uzyskaniu wiarygodnej wiadomości o bezprawnym charakterze danych). Zarazem, zgodnie z art. 15 ustawy o świadczeniu usług drogą elektroniczną, provider nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych. W odniesieniu do dostawców usług udostępniania treści online, analizowana dyrektywa z 17 kwietnia 2019 roku wprowadza nowe zasady odpowiedzialności w związku z czynnościami publicznego udostępniania/podawania do publicznej wiadomości, w zakresie określonym w art. 17 przedmiotowej dyrektywy. Zatem nowe zasady odpowiedzialności nie będą obejmowały na przykład odpowiedzialności za komentarze użytkowników na forum naruszające dobra osobiste osoby trzeciej – w tym zakresie i w innych nie objętych regulacją dyrektywy 2019/790, zastosowanie znajdą dotychczasowe zasady odpowiedzialności określone w art. 14 i 15 ustawy o świadczeniu usług drogą elektroniczną.

Wracając do nowych zasad odpowiedzialności, to wskazać należy, iż art. 17 ust. 4 dyrektywy 2019/790 zawiera katalog działań, jakie dostawcy usług udostępniania sieci online powinni podjąć, aby nie ponosić odpowiedzialności za nieobjęte zezwoleniem czynności publicznego udostępniania treści chronionych prawem autorskim. Zgodnie z przedmiotową normą prawną „jeżeli nie udzielono zezwolenia, dostawcy usług udostępniania treści online ponoszą odpowiedzialność za nieobjęte zezwoleniem czynności publicznego udostępniania, w tym podawania do wiadomości publicznej, chronionych prawem autorskim utworów i innych przedmiotów objętych ochroną, chyba że wykażą, że: a) dołożyli wszelkich starań, aby uzyskać zezwolenia; oraz b) dołożyli wszelkich starań – zgodnie z wysokimi standardami staranności zawodowej w sektorze – aby zapewnić brak dostępu do poszczególnych utworów i innych przedmiotów objętych ochroną, w odniesieniu do których podmioty uprawnione przekazały dostawcom usług odpowiednie i niezbędne informacje; oraz w każdym przypadku c) działali niezwłocznie po otrzymaniu odpowiednio uzasadnionego zastrzeżenia od podmiotów uprawnionych w celu zablokowania dostępu do utworów lub innych przedmiotów objętych ochroną, których dotyczy zastrzeżenie, lub usunięcia ich ze swoich stron internetowych, a także dołożyli wszelkich starań, aby zapobiec ich przyszłemu zamieszczaniu zgodnie z lit. b".

Przy dokonywaniu oceny, czy dany dostawca usług spełnia obowiązki, o których mowa w przytoczonej wyżej normie prawnej oraz w świetle zasady proporcjonalności, należy, między innymi wziąć pod uwagę rodzaj, odbiorców i skalę świadczonych usług oraz rodzaj utworów lub innych przedmiotów objętych ochroną zamieszczanych przez użytkowników usługi oraz dostępność odpowiednich i skutecznych środków, oraz ich koszt dla dostawców usług.

Zatem art. 17 ust. 4 analizowanej dyrektywy zawiera nowe przesłanki wyłączenia odpowiedzialności dostawców usług online. Warto w tym miejscu zwrócić uwagę na art. 17 ust. 8 dyrektywy, zgodnie z którym: „Stosowanie niniejszego artykułu nie wywołuje skutku w postaci ogólnego obowiązku w zakresie nadzoru". Pozornie zatem mogłoby się wydawać, że regulacja ta powtarza jeden do jednego dotychczasową zasadę, iż provider nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych. Warto natomiast w tym zakresie odnieść się do preambuły dyrektywy 2019/790. Zgodnie z jej punktem 66 „Ponadto obowiązki ustanowione w niniejszej dyrektywie nie powinny prowadzić do nakładania przez państwa członkowskie ogólnego obowiązku w zakresie nadzoru. Przy dokonywaniu oceny, czy dostawca usług udostępniania treści online dołożył wszelkich starań zgodnie z wysokimi standardami staranności zawodowej w sektorze, należy wziąć pod uwagę to, czy dostawca usług podjął wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów lub innych przedmiotów objętych ochroną na swojej stronie internetowej, przy uwzględnieniu najlepszych praktyk stosowanych w sektorze i skuteczności podjętych kroków w świetle wszystkich istotnych czynników i rozwoju sytuacji oraz zasady proporcjonalności.



Na potrzeby tej oceny należy wziąć pod uwagę pewną liczbę elementów, takich jak skalę świadczonych usług, rozwijający się zakres istniejących środków, w tym ewentualne przyszłe zmiany, aby unikać dostępności różnych rodzajów treści i kosztów takich środków dla usług. Różne środki mające na celu unikanie dostępności nieobjętych zezwoleniem treści chronionych prawem autorskim mogą być odpowiednie i proporcjonalne w zależności od rodzaju treści, w związku z czym nie można wykluczyć, że w niektórych przypadkach dostępności nieobjętych zezwoleniem treści można uniknąć jedynie po powiadomieniu podmiotów uprawnionych. Wszelkie kroki podejmowane przez dostawców usług powinny być skuteczne w odniesieniu do zamierzonych celów, lecz nie powinny wykraczać poza to, co jest konieczne do osiągnięcia celu, jakim jest unikanie i zaprzestanie dostępności nieobjętych zezwoleniem utworów i innych przedmiotów objętych ochroną".

Z powyższego można wywieść, iż co prawda ogólnego obowiązku nadzoru nad treściami umieszczanymi w serwisie przez użytkowników nie ma, jednak każdy właściciel serwisu powinien podjąć wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów i innych przedmiotów objętych ochroną na swojej stronie internetowej, przy uwzględnieniu najlepszych praktyk stosowanych w sektorze i skuteczności podjętych kroków w świetle wszystkich istotnych czynników i rozwoju sytuacji oraz zasady proporcjonalności. Na potrzeby tej oceny należy wziąć pod uwagę pewną liczbę elementów, takich jak skalę świadczonych usług, rozwijający się zakres istniejących środków, w tym ewentualne przyszłe zmiany, aby unikać dostępności różnych rodzajów treści i kosztów takich środków dla usług. Różne środki mające na celu unikanie dostępności nieobjętych zezwoleniem treści chronionych prawem autorskim mogą być odpowiednie i proporcjonalne w zależności od rodzaju treści, w związku z czym nie można wykluczyć, że w niektórych przypadkach dostępności nieobjętych zezwoleniem treści można uniknąć jedynie po powiadomieniu podmiotów uprawnionych. Wszelkie kroki podejmowane przez dostawców usług powinny być skuteczne w odniesieniu do zamierzonych celów, lecz nie powinny wykraczać poza to, co jest konieczne do osiągnięcia celu, jakim jest unikanie i zaprzestanie dostępności nieobjętych zezwoleniem utworów i innych przedmiotów objętych ochroną".

Z powyższego można wywieść, iż co prawda ogólnego obowiązku nadzoru nad treściami umieszczanymi w serwisie przez użytkowników nie ma, jednak każdy właściciel serwisu powinien podjąć wszystkie kroki, jakie podjąłby staranny podmiot dla osiągnięcia celu dotyczącego zapobiegania dostępności nieobjętych zezwoleniem utworów. Nowe regulacje zatem „zmiękczają" nieco brak ogólnego obowiązku nadzoru, kładąc nacisk na pewien obowiązek podejmowania przez hosting providerów działań prewencyjnych i stosownych aktów staranności. Zatem optyka w kontekście wyłączenia odpowiedzialności hosting providera w związku z brakiem obowiązku nadzoru jest już inna.

Podsumowanie

Nowe regulacje mają na celu dalsze wzmocnienie ochrony twórców. Dyrektywa 2019/790 stawia nowe wyzwania dla hosting providerów wpadających w definicję dostawcy usług udostępniania treści online. Model biznesowy takich dostawców będzie wymagał odpowiedniego przemodelowania w związku z nowymi regulacjami. Czasu na przygotowania jeszcze trochę zostało, zwłaszcza, iż w pierwszej kolejności trzeba poczekać na rodzime regulacje, które implementują zapisy omawianej dyrektywy do polskiego porządku prawnego.