

Sponsorowany przez:
Cisco Systems
EXATEL

Autor:
Jarosław Smulski

Marzec, 2019



Bezpieczna sieć bezprzewodowa jest równie istotna, jak bezpieczna sieć LAN. A w przyszłości będzie nawet ważniejsza, ponieważ to bezprzewodowy dostęp do sieci będzie podstawowym modelem korzystania z internetu.



Sieć bezprzewodowa WLAN niezbędnym elementem polityki bezpieczeństwa IT każdej organizacji.

Poznaj wyniki badania IDC oraz trendy rynkowe

WSTĘP

„Kabel to kabel” – to jedna z wypowiedzi, jakie usłyszeli analitycy IDC prowadzący na przełomie 2018 i 2019 roku badanie dotyczące modeli używania sieci bezprzewodowych w Polsce. Można tę wypowiedź traktować jako przejaw odpowiedzialności za bezpieczeństwo infrastruktury IT, poprzez eliminowanie



2/3

BADANYCH

ORGANIZACJI UDOSTĘPNIA
PRACOWNIKOM LUB
GOŚCIOM/KLIENTOM SIEĆ
WiFi

technologii, do których nie mamy do końca zaufania. Czy dzięki temu dana organizacja będzie rzeczywiście bezpieczniejsza? Czy będzie potrafiła wyśledzić punkt dostępu podszywający się pod daną instytucję? Czy pracownikom wystarczy tani internet w telefonach komórkowych, aby poprawić ich efektywność?

Nic bardziej mylnego. Tani internet w telefonach komórkowych między innymi dlatego jest tani, że jego poziom bezpieczeństwa jest

wystarczający raczej dla konsumentów czy małych przedsiębiorstw. Czy na taką niefrasobliwość mogą sobie pozwolić na przykład podmioty zarządzające infrastrukturą strategiczną dla kraju? Czy dostęp do Internetu mobilnego udostępniony w dobrej wierze przez niefrasobliwego pracownika, nie staje się groźną luką w klasycznych zabezpieczeniach, na które wydano niebagatelne sumy? Bezpieczna sieć bezprzewodowa jest obecnie równie istotna, jak bezpieczna sieć LAN. A w przyszłości będzie nawet ważniejsza, ponieważ to bezprzewodowy dostęp do sieci będzie podstawowym modelem korzystania z internetu.



Aż 41% respondentów twierdzi, że rozwiązania bezprzewodowe budują pozytywny wizerunek organizacji.

48%

ORGANIZACJI MONITORUJE
SWOJĄ PRZESTRZEŃ
RADIOWĄ

organizacji może ją uchronić od ataku hackerskiego czy innych naruszeń bezpieczeństwa sieci IT. Tymczasem, u ponad połowy respondentów badania (52%) takie praktyki nie są w ogóle wprowadzane.

Sieci WLAN można wykorzystać na wiele różnych sposobów wychodzących poza stereotypowy dostęp do Internetu, a producenci tego typu rozwiązań prześcigają się wręcz w opracowywaniu nowych. Czy mamy więc z nich rezygnować w imię złe rozumianego poczucia bezpieczeństwa? Oczywiście, że nie: badania oraz praktyki pokazują, że tylko pełne monitorowanie przestrzeni radiowej

87%

RESPONDENTÓW OCZEKUJE, ŻE
WIFI SAMO W SOBIE BĘDZIE
BEZPIECZNE I ZAPEWNI
BEZPIECZEŃSTWO

w sobie będą bezpieczne i zapewnią bezpieczeństwo. Dopiero na drugim miejscu, z 74% wskazań, jest kryterium wydajności tych urządzeń sieciowych.

Wspomniane wyżej badanie IDC pokazuje, że kwestie bezpieczeństwa są bardzo istotne dla polskich użytkowników, chociaż często nie wykorzystują oni możliwości, jakie dają współczesne rozwiązania WLAN. Jednak nie tolerują oni rozwiązań, które byłyby zagrożeniem dla bezpieczeństwa danej organizacji. Aż 87% respondentów oczekuje, że rozwiązania bezprzewodowe same

Katalog możliwych rozwiązań wykorzystania sieci WiFi jest obszerny i sięga od hasel inteligentnego budynku (nawigacja wewnątrz budynku, zarządzanie różnymi aktywnościami), poprzez wsparcie systemów obsługi klientów, aż po rozwiązania ze świata Smart City. Wszystkie one budują pozytywny wizerunek nowoczesnej organizacji, na co zwróciło uwagę 41% respondentów.

SPIS TREŚCI

WSTĘP	1
W TYM DOKUMENCIE	4
TECHNOLOGIA WLAN Niezbędnym elementem transformacji cyfrowej	4
<i>Skanowanie przestrzeni radiowej to najskuteczniejsza polityka bezpieczeństwa</i>	5
<i>Bezpieczeństwo wpływa na modele zastosowania WiFi</i>	7
<i>Smart City</i>	8
PODSUMOWANIE	9

SPIS ILUSTRACJI

Ryc. 1 Bezpieczna sieć WiFi jest odseparowana i autoryzująca dostęp użytkowników	6
Ryc. 2 Sieć WiFi to ułatwienie w pracy dla pracowników, klientów i gości	7
Ryc. 3 Sieci WiFi często wykorzystywane w projektach Smart City w Polsce	



Organizacje wstrzymujące inwestycje w nowoczesne sieci bezprzewodowe, czy to ze względu na źle rozumiane bezpieczeństwo, czy też nie znając przekonujących przykładów budowy nowych usług, ograniczają pracownikom dostęp do potrzebnych narzędzi i danych, krępują ich kreatywność.

W TYM DOKUMENCIE

Ten dokument opisuje zalety technologii WLAN oraz jej znaczenie dla poprawy bezpieczeństwa informatycznego organizacji reprezentujących administrację publiczną, sektor bankowy, energetyczny i transport. Prezentuje również różne innowacyjne modele jej wykorzystania oraz ich percepcję wśród przedstawicieli różnych branż.

Dokument został napisany na bazie ankiet przeprowadzonych w Polsce metodą CATI wśród dyrektorów, kierowników oraz specjalistów odpowiedzialnych za infrastrukturę IT albo sieciową w organizacjach z tych wybranych branż.

TECHNOLOGIA WLAN NIEZBĘDNYM ELEMENTEM TRANSFORMACJI CYFROWEJ

Technologia bezprzewodowych sieci oraz bezprzewodowego dostępu do Internetu w ciągu zaledwie kilkunastu lat stała się powszechnym standardem. Tak powszechnym, że przestajemy w nim upatrywać rozwiązań, które mogą przynosić nowe, innowacyjne usługi dla biznesu. Tymczasem analitycy IDC wyraźnie wskazują, że infrastruktura WLAN jest bardzo istotnym elementem budowy strategii transformacji cyfrowej (Digital Transformation; DX), która umożliwia budowę rozwiązań opartych na IoT, wielokanałowej sprzedaży (Omnichannel), czy dostępu do krytycznych dla biznesu aplikacji w modelu SaaS bez żadnych ograniczeń. Zresztą świat dostawców tej technologii szybko się dostosowuje do nowych zasad gry, promując na przykład narzędzia zarządzania środowiskiem sieciowym w chmurze.

Organizacje wstrzymujące inwestycje w nowoczesne sieci bezprzewodowe, czy to ze względu na źle rozumiane bezpieczeństwo, czy też nie znając przekonujących przykładów budowy nowych usług, ograniczają pracownikom dostęp do potrzebnych narzędzi i danych, krępują ich kreatywność, skazując na spetryfikowane modele pracy stanowiskowej. Takie organizacje wolniej się rozwijają, są mniej innowacyjne, a często także przegrywają wyścig o cennego pracownika, dla którego bezprzewodowy model pracy jest standardem.

Warto w tym miejscu zaprezentować kilka liczb. Mimo tego, że badanie częściowo dotyczyło raczej konserwatywnych branż, takich jak administracja centralna



AŻ 84%

PRACOWNIKÓW KORZYSTA ZE
SŁUŻBOWYCH URZĄDZEŃ
MOBILNYCH

i terytorialna, to aż 60% respondentów wskazało, że zatrudnia pracowników, których praca przy wykorzystaniu urządzeń mobilnych (np. laptop) może być wykonywana z więcej niż jednej lokalizacji. Co więcej, aż 84,5% pracowników korzysta ze

służbowych urządzeń mobilnych, a 68,5% organizuje spotkania w przeznaczonych do tego celu pomieszczeniach (sale konferencyjne), w których zachodzi potrzeba używania takich urządzeń. Tylko w stosunku do polityki Bring Your Own Device jest



Małe instalacje (od 1 do 19 punktów) stanowią aż 77% przebadanych podmiotów.

bardzo duża nieufność wywołana przez kwestie bezpieczeństwa i trudności w zarządzaniu takim sprzętem, co przekłada się na to, że tylko 19% respondentów zezwala na takie praktyki.

Aby jednak rozpocząć podróż w kierunku organizacji, w której bezprzewodowa sieć jest oczywistością, należy zdefiniować na nowo kwestię bezpieczeństwa IT oraz postawić ją na piedestale. Nowocześnie rozumiane bezpieczeństwo jest bowiem podstawą każdej strategii transformacji cyfrowej.

Skanowanie przestrzeni radiowej to najsukuteczniejsza polityka bezpieczeństwa

Badanie IDC wykazało, że 2/3 polskich organizacji udostępnia pracownikom lub gościom/klientom sieć WiFi, mimo różnych zastrzeżeń co do bezpieczeństwa tego typu rozwiązań. Aż w 95,5% przypadków sieć WiFi jest przeznaczona do użytku pracowników, a w 73,5% udostępniana jest gościom danej organizacji. Duża grupa respondentów stara się jednak ograniczać jej użytkowanie poprzez oddzielenie tej sieci od całej infrastruktury sieciowej; najczęściej też sieć ta jest dostępna tylko w niektórych, wybranych pomieszczeniach (sale konferencyjne, gabinety osób zarządzających). Stosunkowo duża grupa podmiotów (16,7%) dysponuje tylko jednym punktem dostępu do sieci bezprzewodowej, a małe instalacje (od 1 do 19 punktów) stanowią aż 77,3% przebadanych podmiotów. Dlatego też jako standardowy model dostępu do Internetu na sieć bezprzewodową wskazało zaledwie 7,1% respondentów. W większości przypadków sieć WLAN ma charakter komplementarny a pracownicy na co dzień korzystają z sieci LAN.

Jakie metody zabezpieczenia są najczęściej stosowane? Najczęściej respondenci starają się fizycznie odseparować sieć bezprzewodową od sieci LAN (78,8%



52%

RESPONDENTÓW NIE
IDENTYFIKUJE I NIE
MONITORUJE ZAGROŻENIA
W PRZESTRZENI RADIOWEJ

przypadków). Taka strategia ograniczania strat poprzez wydzielenie, jakby z góry zakłada, że do takiego naruszenia bezpieczeństwa prędzej czy później dojdzie. Co więcej, nie jest stuprocentowa bezpieczna, ponieważ nie jesteśmy w stanie zapewnić idealnej separacji obu środowisk. W sposób oczywisty ogranicza również produktywność pracowników, nie dając

im możliwości korzystania z aplikacji czy danych biznesowych, ograniczając rolę sieci bezprzewodowej do prostego dostępu do Internetu.

Taki sam odsetek wskazał na używanie różnych metod uwierzytelniania oraz autoryzowania dostępu użytkowników do WiFi. Są to oczywiście sposoby skopiowane z rozwiązań przewodowych; dobrze wprowadzone i przestrzegane zapewniają dużą pewność, że dostęp do sieci będzie autoryzowany oraz zamknięty dla osób niepowołanych. Jednak radiowy charakter sieci bezprzewodowych zmusza administratorów do szerszego spojrzenia na ten problem i uwzględnienie tej specyfiki. Niestety ponad połowa respondentów (51,5%) nie identyfikuje i nie monitoruje



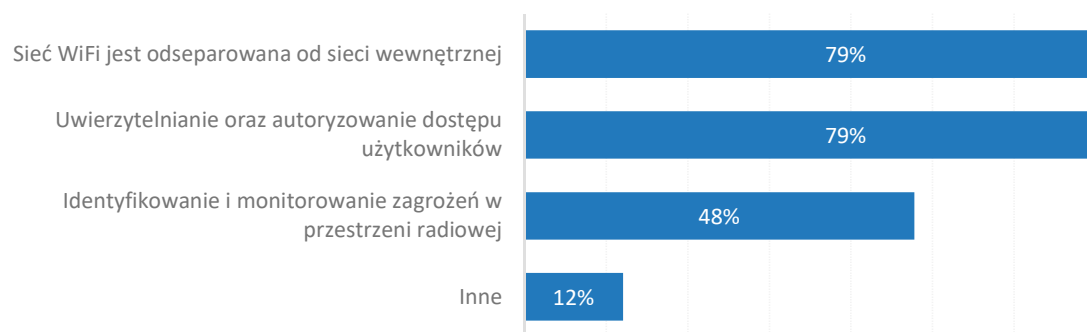
Zdecydowanie większym zagrożeniem jest pojawienie się w przestrzeni radiowej punktu udającego w nazwie autoryzowany punkt danej organizacji. Nieświadomi tego pracownicy wykorzystują takie punkty mając zaufanie, że jest to bezpieczny punkt pod kontrolą administratorów IT i tym samym wystawiają cenne dane na kradzież.

zagrożenia w przestrzeni radiowej. Mimo tego, że jest to zdecydowanie najbardziej skuteczna i proaktywna metoda wykrywania niebezpiecznych zdarzeń w sieci. A takie zagrożenie mogą również tworzyć sami pracownicy, uruchamiając swoje własne, nieautoryzowane punkty dostępowe. Aż 22% wszystkich respondentów, w tym też tych, którzy nie posiadają sieci WiFi, spotkało się z takim naruszeniem zasad bezpieczeństwa.

RYC. 1

Bezpieczna sieć WiFi jest odseparowana i autoryzująca dostęp użytkowników

Q6. Jakie element zabezpieczeń sieci WiFi Państwo posiadają?



Uwaga: N = 132

Źródło: IDC, 2019

Zdecydowanie większym zagrożeniem jednak jest pojawienie się w przestrzeni radiowej punktu udającego w nazwie autoryzowany punkt dostępu danej organizacji. Nieświadomi tego pracownicy wykorzystują takie punkty, mając zaufanie, że są one

DOŚWIADCZENIA RESPONDENTÓW

22% WSZYSTKICH

RESPONDENTÓW SPOTKAŁO SIĘ
Z TWORZENIEM PRYWATNYCH
PUNKTÓW DOSTĘPU PRZEZ
PRACOWNIKÓW

AŻ 4%

WSZYSTKICH RESPONDENTÓW
DOŚWIADCZYŁO PUNKTU
DOSTĘPU UDAJĄCEGO
AUTORYZOWANY PUNKT
DANEJ ORGANIZACJI



Sieć WiFi przede wszystkim ma służyć ułatwieniu w pracy pracownikom oraz klientom i gościom danej organizacji.

bezpieczne pod kontrolą administratorów IT i tym samym wystawiają cenne dane na kradzież, a same urządzenia po zainfekowaniu mogą stać się końmi trojańskimi, otwierającymi dostęp do sieci LAN, nawet jeśli w danym środowisku nie ma sieci WLAN. Z takimi przypadkami spotkało się 3,5% respondentów.

To zagrożenie jest w szczególności niebezpieczne dla podmiotów zajmujących się strategiczną infrastrukturą dla kraju, które aby uniknąć takich ataków, powinny decydować się na szeroko zakrojony projekt oparcia bezpieczeństwa właśnie na sieciach bezprzewodowych z zaawansowanymi narzędziami skanującymi przestrzeń radiową. Niestety takie podejście, w którym funkcją sieci bezprzewodowej jest zapewnienie bezpieczeństwa IT całego środowiska jest stosunkowo rzadkie; zostało wybrane przez zaledwie 16% respondentów.

Bezpieczeństwo wpływa na modele zastosowania WiFi

Świadomość ewentualnych zagrożeń niestety wpływa też na chęć wykorzystywania WiFi do innych celów. Zdecydowana większość respondentów (65,2%) wskazuje, że sieć ta ma służyć ułatwieniu w pracy pracownikom oraz klientom i gościom danej organizacji (61,4%). Na trzecim miejscu są korzyści wizerunkowe – kształtowanie wizerunku nowoczesnej, przyjaznej dla klientów organizacji (40,9%). Inne przykłady zastosowania sieci bezprzewodowych były wymieniane zdecydowanie rzadziej. Pokazuje to potrzebę dalszej edukacji użytkowników tej technologii w Polsce, w szczególności biorąc pod uwagę nadchodzące zmiany, jakie nastąpią po upowszechnieniu się rozwiązań IoT.

RYC. 2

Sieć WiFi to ułatwienie w pracy dla pracowników, klientów i gości

Q10. Jakie korzyści przynosi Państwa organizacji wykorzystanie sieci bezprzewodowej?



Uwaga: N = 132

Źródło: IDC, 2019

Co ciekawe, gdy to samo pytanie zostało zadane organizacjom, które nie posiadają jeszcze WiFi, to aż 57,4% nie potrafiło wskazać żadnej odpowiedzi, a 22,1% odpowiedziało, że poprawi to wizerunek danego podmiotu. Dowodzi to tego, że



Zaledwie 17% respondentów reprezentujących samorządy, może się pochwalić projektami Smart City.

brakuje wiedzy, do czego można wykorzystać sieć WiFi, ale jej brak ma negatywny wpływ na wizerunek organizacji.

Organizacje, które potrafiły wyjść poza schemat rozumienia WiFi, jako usługi komplementarnej komunikacji do dostępu „po kablu” uruchomiły szereg często bardzo wyspecjalizowanych usług, które pozwoliły sprostać nowym wyzwaniom narzuconym przez przepisy czy konkurencję.

Przykładem interesującego wdrożenia sieci kampusowych jest sieć bezprzewodowa rozciągnięta na dwa kampusy służb miejskich w Amsterdamie, liczące ponad 50 budynków. Odpowiednio przeprowadzone wdrożenie nie tylko zapewnia wysokiej jakości dostęp do Internetu w każdym budynku i na wspólnym terenie, bezpieczną, centralnie zarządzaną infrastrukturę, ale również spore oszczędności, ponieważ nowa sieć bezprzewodowa umożliwiła konsolidację posiadanej przestrzeni biurowej. To nie tylko następny ciekawy przykład budowy nowoczesnej infrastruktury dla samorządu, ale również projekt wkraczający już w świat Smart City.

Smart City

Mimo ożywionej dyskusji na temat Smart City w Polsce, zaledwie 17,1% respondentów reprezentujących samorządy, może się pochwalić projektami, które można zaliczyć do spełniających definicję tej strategii. Jednak wśród tych samorządów, które jeszcze nie wdrażały takich projektów, 27% właśnie wdraża albo ma takie plany. Jest to dowód na rosnące zainteresowanie polskich samorządów takimi projektami. Najczęściej wykorzystują one połączenia komórkowe (56,7%) oraz stacjonarne (53,3%) a jako trzecia najpopularniejsza odpowiedź były wymieniane technologie krótkodystansowe takie jak Bluetooth, Zigbee, czy WiFi (40%). Tyle samo samorządów wdrażających projekty Smart City, zdecydowało się na technologie bezprzewodowe LPWAN (NB-IoT, LoRa, SigFox).

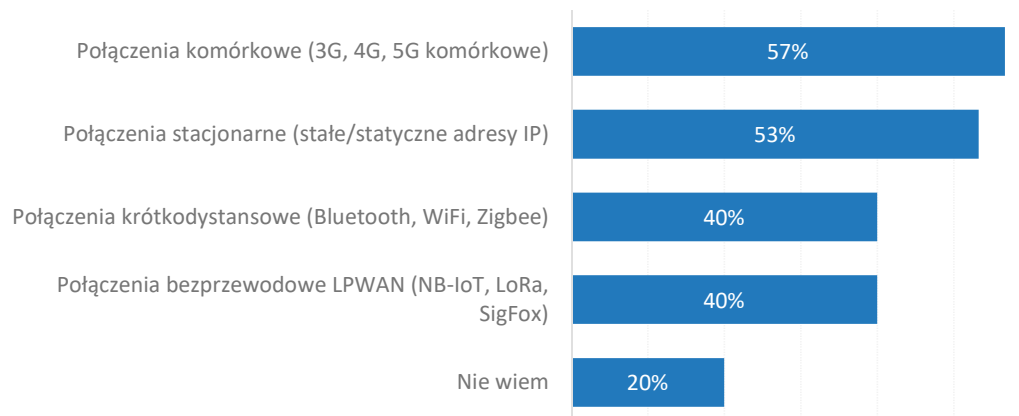


Sieci WiFi, jak inne połączenia krótkodystansowe, są stosunkowo często wykorzystywane w projektach Smart City.

RYC. 3

Sieci WiFi często wykorzystywane w projektach Smart City w Polsce

Q11C. Jakie technologie komunikacyjne wykorzystują Państwo lub zamierzają wykorzystać w tych projektach?



Uwaga: N = 30

Źródło: IDC, 2019

Jeśli chodzi o zakres geograficzny tych projektów, to aż 70% z nich jest rozciągnięta na całe miasto. Najmniejsze projekty kampusowe stanowią drugą grupę mającą 16,7%. Oznacza to, że projekty Smart City są mocno osadzone w strategii rozwoju polskich miast; są to projekty kompleksowe, skomplikowane o dużych budżetach.

Katalog możliwych modeli wykorzystywania WiFi w wdrożeniach Smart City jest bardzo bogaty, a ponieważ polskie miasta dysponują już całkiem sporą infrastrukturą sieciową, można ją wykorzystać do nowych zastosowań, wychodząc poza proste funkcje dostarczania darmowych, miejskich hot-spotów.

PODSUMOWANIE

Badanie przygotowane przez IDC we współpracy z Cisco Systems i EXATEL dobitnie pokazuje, że dyrektorzy, kierownicy działów IT wybranych sektorów potrzebują edukacji oraz przykładów wdrożeń WLAN. Z jednej strony szybko zmieniają się modele pracy w kierunku pracowników mobilnych, którzy potrzebują dostępu do danych i aplikacji biznesowych o każdej porze i w każdym miejscu. A z drugiej strony źle przygotowana polityka bezpieczeństwa prowadzi do ograniczania zasięgu sieci bezprzewodowych, pozbawiając pracowników dodatkowych narzędzi.

Kwestie właściwie rozumianego bezpieczeństwa są najważniejsze w zmianie percepcji tej technologii. Potrzeba ich zredefiniowania – z elementu zagrażającego bezpieczeństwu IT, musi stać się jej najważniejszym elementem, gwarantem bezpiecznej komunikacji w biznesie i administracji publicznej.

Szefowie działów IT potrzebują również inspiracji, w jaki sposób dzięki WiFi budować nowoczesne, innowacyjne usługi dla biznesu czy obywateli. Sieć bezprzewodowa ma bowiem olbrzymi potencjał i jest bez wątpienia niezbędnym elementem budowy strategii transformacji cyfrowej. Takim, który nie tylko daje pracownikom nowe narzędzia pracy, ale także umożliwia kreowanie cyfrowych produktów i usług dla klientów. A to jest właśnie istotą transformacji cyfrowej.

O IDC

International Data Corporation (IDC) jest jedną z największych firm zajmujących się badaniem rynku teleinformatycznego oraz twórcą wielu analiz sektorowych, a także strategicznym doradcą w wielu projektach. Głównym zadaniem firmy jest dostarczanie analiz na temat przyszłych trendów rozwojowych poszczególnych sektorów rynku. Obecnie dla IDC pracuje ponad 1100 analityków w 110 krajach. Klientami IDC są czołowe firmy IT, organizacje badawcze oraz instytucje finansowe. Od ponad 50 lat prezesi, dyrektorzy oraz kierownicy działów informatycznych polegają na badaniach oraz analizach przygotowywanych przez ekspertów IDC. IDC jest częścią IDG, światowego lidera w dziedzinie wydawnictw dla profesjonalistów branży informatycznej.