Ostatnia aktualizacja: 09/ 2011

CC Otwarte Systemy Komputerowe
Bezpieczne sieci WiFi

Sieci WiFi – rozwój i zagrożenia

Bezprzewodowe sieci lokalne zyskują coraz większą popularność w zastosowaniach biznesowych. Wydajność dostępnych rozwiązań rośnie - obecnie oferowane są już punkty dostępowe generacji „n" o przepustowościach dochodzących do 600Mbps. Rośnie też liczba wdrożeń różnych rozwiązań pochodnych takich jak np. smartphone-ów, mobilnych systemów telefonii VoIP, itd. Rosnąca liczba wdrożeń nie idzie jednak w parze ze zwiększeniem bezpieczeństwa rozwiązań bezprzewodowych. W branży panuje dość powszecha opinia, że pod względem bezpieczeństwa danych technologie bezprzewodowe pozostają w tyle za tradycyjnymi technologiami „kablowymi". Opinie te są w dużym stopniu prawdziwe – do najistotniejszych zagrożeń związanych z sieciami bezprzewodowymi zaliczyć można:

- Otwartość medium komunikacji sprawia że z założenia sieć bezprzewodowa jest bardziej narażona na „podsłuch", gdyż nie wymaga fizycznego dostępu do sieci (ruch można np. podsłuchać z parkingu przed biurem lub z innego piętra)
- Stosowane standardy zabezpieczeń takiej jak np. WEP są przestarzałe, mimo to w dalszym ciągu używane, co powoduje, że zabezpieczenia kryptograficzne przy obecnym dostępnym sprzęcie są trywialne do przełamania
- Wiele implementacji standardowych protokołów i algorytmów posiada różnego rodzaju błędy, które powodują, że nawet silne zabezpieczenia można obejść
- Nieznajomość nowej technologii powoduje, że wielu administratorów popełnia kardynalne błędy wdrażając systemy bezprzewodowe (np. pozostawiając domyślne hasła, itp.).
- Sieci bezprzewodowe stwarzają nowe możliwości szpiegostwa przemysłowego i wycieków danych, nawet w przypadku gdy sieć firmowa jest poprawnie zabezpieczona – np. zestawione ad-hoc połączenie pomiędzy siecia LAN a osobą znajdującą się fizycznie poza firmą pozwala na przesłanie znacznej ilość danych w krótkim czasie.

Bezpieczeństwo i inne problemy związane z wdrażaniem sieci WiFi

Oto najważniejsze kwestie związane z zagrożeniami jakie stwarzają sieci WiFi:

- **Otwarte punkty dostępowe** – takie rozwiązanie stosowane np. w publicznie dostępnych sieciach miejskich nie powino funkcjonować w zastosowaniach bieznesowych. Niektórzy producenci dostarczają jednak sprzęt skonfigurowany domyślnie jako otwarty AP.
- **Przestarzałe protokoły kryptograficzne** – metody zabezpieczeń takie jak WEP czy pierwsze wersje WPA pozwalają na proste odszyfrowanie i przejęcie kontroli nad ruchem siecowym, mimo to są w dalszym ciągu stosowane, zwłaszcza w przypadku starszego sprzetu i oprogramowania

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

- **Domyślne hasła i SSID** – pozostawienie domyślnych SSID i haseł producentów powoduje, że sieć bezprzewodowa jest praktycznie całkowicie otwarta na podsłuch
- **Błędy w oprogramowaniu** – nawet odpowiednio mocne zabezpieczenia kryptograficzne mogą być pokonane w przypadku błędów w implementacji, sytuacje takie wiele razy występowały w oprogramowaniu punktów dostępowych różnych producentów
- **„Rogue Access Point"** - nawet w przypadku dobrze zabezpieczonej sieci lub w przypadku gdy firma nie stosuje technologi WiFi punkt dostepowy podłączony do sieci LAN przez nieautoryzowaną osobę (np. w miejsce komputera stacjonarnego) może być wykorzystany do przechywcenia części ruchu sieciowego lub do uzyskania dostępu do komputerów pracowników (zwłaszcza notebooków).
- **Wirless uplink** – połączenie typu ad hoc zestawione między komputerem podłączonym do sieci lokalnej a komputerem poza firmą może być wykorzystane do transmisji poufnych danych na zewnątrz firmy. Ten scenariusz może być zrealizowany zarówno poprzez klasycznego sprziega przemysłowego jak i przez nieświadomego pracownika, którego komputer został przejęty przez hackera

Prócz kwestii związanych ściśle z zagrożeniami stwarzanymi przez hackerów istnieje szereg innych problemów utrudniających integrację sieci bezprzewodowych z istniejącą infrastrukturą, wymienić tu można:

- Zapewnienie właściwego pokrycia zasięgiem sieci, uniknięcie interferencji a także martwych stref
- Zapewnienie kontroli dostępu w wydzielonych wirtualnych strefach: np. dostęp dla gości powinien być ograniczony do dostępu internetowego, pracownicy tymczasowi powinni dodatkowo posiadać dostęp do poczty elektronicznej i wybranych serwisów intranetowych a uprawnienia pracowników etatowych powinny pokrywać się z uprawnieniami jakie posiadają w tradycyjnej sieci
- Zapewnienie właściwej przepustowości - mimo rozwoju technologii sieci WiFi są w dalszym ciągu wolniejsze od tradycyjnego kablowego Ethernetu. Jednocześnie przepustowości pojedynczych AP są dość ograniczone co może stwrarzać problemy w przypadku jednoczesnego wykorzystania punktu dostępowego przez wiele osób np. w sali konferencyjnej
- Wyróżnienie rodzajów ruchu sieciowego i nadanie mu odpowiednich priorytetów, co nabiera szczególnego znaczenia np. w przypadku telefonii VoIP
- Zapewnienie niezawodności połączeń, także w przypadku awarii sprzętu
- Tak jak każdy kolejny system IT WLAN zwiększa obowiązki personelu administracji IT oraz help-desk, wskazane są więc rozwiązania maksymalnie odciążające personel IT

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

Od czego zacząć?

Wybór rozwiązania bezprzewodowego należy rozpocząć od sformułowania kilku podstawowych pytań technicznych oraz biznesowych:

- Ilu użytkowników bezprzewodowych liczy moja sieć i ilu będzie liczyć za rok?
- Czy mam odziały lub biura regionalne i czy chcę wdrożyć sieć bezprzewodową także w nich? Jak duże i na ile autonomiczne są oddziały?
- Jakie jest fizyczne rozmieszczenie pomieszczeń i gdzie powinna być dostępna sieć WiFi? Czy możliwe jest wyróżnienie obszarów o zwiększonym zapotrzebowaniu na dostęp do sieci?
- Czy sieć bezprzewodowa będzie dostępna w pomieszczeniach niebiurowych – tj. np. w halach produkcyjnych lub na otwartym powietrzu albo też w obszarach cechujących się szczególnie trudnymi warunkami środowiskowymi (wysoka lub niska, temperatura, itp)? Czy konieczne będzie zastosowanie punktów dostępowych o podwyższonej odporności na wpływy środowiska?
- Czy poziom uprawnień użytkowników będzie zóżnicowany? Czy chcemy rozgraniczyć uprawnienia pracowników, gości, pracowników sezonowych, itp. ?
- Czy rozważamy wykorzystnie bezporzewodowego VoIP (VoWLAN)?
- Jak będa autoryzowani użytkownicy? Czy wymagana będzie integracja z domeną Windows, systemem VPN, itp.?
- Na ile istotne są dla nas zagrożenia związane z utratą poufnych danych / szpiegostwem przemysłowym? Czy chcemy wykrywać tego typu zagrożenia i automatycznie reagować na nie?

Przed rozpoczęciem wyboru producenta systemu wireless powinniśmy przygotować następującą (lub podobną) tabelkę:

• Całkowita liczba użytkowników w centrali i ew. oddziałach • Liczba oddziałów w których ma być wdrożony WLAN	_____ _____
Powierzchnia przestrzeni biurowej i innej, na której ma być wdrożona sieć WiFi	_____
Czy jest wymagana autoryzacja domeny lub podobna?	[TAK] [NIE]
Czy mają być zastosowane zróżnicowane uprawnienia ?	[TAK] [NIE]
Czy będzie wdrożony VoWLAN (VoIP na WiFi)?	[TAK] [NIE]
Czy wymagane będzie raportowanie z wykorzystania sieci WLAN?	[TAK] [NIE]
Czy chcemy wykrywać i automatycznie reagować na zagrożenia takie jak „Rogue AP”	[TAK] [NIE]

Dostępne rozwiązania

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/

Poniżej podsumowaliśmy najważniejsze cechy oferowanych przez nas rozwiązań WiFi:

Producent	Cechy
Ruckus Wireless	Sprzęt klasy „Enterprise" oferujący zcentralizowane zarządzanie, dodatkowo nowatorskie rozwiązania z dziedziny technologii nadawczo-odbiorczej powodują, że pojedynczy AP Ruckus jest w stanie wydajniej obsłużyć większą liczbę użytkowników, dzięki czemu liczba AP potrzebnych do pokrycia danego obszaru jest mniejsza niż w przypadku produktów innych firm.
Aruba Networks	Sprzęt klasy Enterprise" oferujący całkowicie zcentralizowane zarządzanie, b. dobra obsługę VOIP szereg funkcji bezpieczeństwa, takichjak firewall i IPS oraz dynamicznie dostosowujacy się do zmiennych cech środowiska pracy – np. dynamicznie alokujący AP w zależności od obciążenia sieci.

Jakiego producenta systemu WiFi wybrać?

Wybór optymalnego systemu bezprzewodowego zależy od oczekiwanej funkcjonalności. Zupełnie innny poziom funkcji zapewniają producenci klasy SoHo oferujący sprzętu w cenie rzędy 50 USD za punkt dostępowy a producenci sprzętu klasy Enterpise pozwalającego na realizacje sieci złożonej z kilkudziesięu do nawet kilkunastu tysięcy punktów dostepowych.

Wielkość firmy	Typowe cechy i wymagania	Propozycja wyboru producenta
SoHo, proste instalacje 1-10 AP (sklepy, gastronomia, małe biura)	• Prosta konfiguracja, prosta administracji, brak integracji z innymi komponentami	• Ruckus Wireless
Do kilkadzięciu AP (biura)	• „captive portal", zcentralizowana administracja, Integracja z usługami katalogowymi, rozdzielenie ról użytkowników	• Ruckus Wireless, Aruba Networks
Kilkaset - tysiące AP	• jw. plus inne funkcje bezpieczeństwa, takie jak wykrywanie włamań, wykrywanie anomalii, skalowalność i wysoka-niezawodność	• Aruba Networks
Sieci metroploitalne i instalacje przemysłowe	• Skalowalność, zcentralizowane zarządzanie, punkty dostepowe odporne na wpływy atmosferyczne	• Ruckus Wireless, Aruba Networks
Radiolinie punkt-punkt	• odporność na błędy transmisji, duży zasięg, łatwość kalibracji wiązki	• Ruckus Wireless

Wybrane referencje CC w zakresie rozwiązań firewall i ochrony danych:

- Auchan Polska sp. z o.o.,
- CA IB S.A.
- Urząd M.st. Warszawa – Ursynów,
- Sodexo Pass Polska Sp z o.o.

ul. Rakowiecka 36
02-532 Warszawa
tel. +48 22 646-68-73
fax +48 22 606-37-80
e-mail:office@cc.com.pl
Web: http://www.cc.com.pl/

- FM Polska Sp z o.o. (FM Logistic)
- Nestle Polska S.A.
- Ministerstwo Sprawiedliwości
- Wojskowa Akademia Techniczna,
- BRE Corporate Finance S.A.,
- WestLB Bank Polska S.A.,
- PBP Bank Polska S.A.
- Provident Polska S.A.,
- RockWool Polska S.A.,
- Uniwersytet Warszawski, Wydział Chemii
- Zelmer

Więcej informacji o firmie znajdziecie Państwo w Internecie, na stronach: **http://www.cc.com.pl/**

Osoby kontaktowe:

Dział Techniczny: tech@cc.com.pl

Dział Handlowy: sales@cc.com.pl

ul. Rakowiecka 36 tel. +48 22 646-68-73 e-mail:office@cc.com.pl
02-532 Warszawa fax +48 22 606-37-80 Web: http://www.cc.com.pl/