Luki w zabezpieczeniach organizacji

Cyberprzestrzeń to infrastruktura współczesnego świata, a cyberbezpieczeństwo to infrastruktura cyberprzestrzeni.

Wprowadzenie

Obecność w Internecie stała się warunkiem działania każdej organizacji, niezależnie od tego, czy jest to agencja rządowa, działalność gospodarcza czy instytucja akademicka. Każda organizacja potrzebuje otwartych drzwi dla społeczeństwa, z możliwością obsługi swojego okręgu wyborczego online i zdolnością do bezpiecznego przechowywania danych. Internet oferuje niespotykane możliwości praktycznie każdej organizacji. Jednak pojawiają się bezprecedensowe niebezpieczeństwa, które mogą prowadzić do kosztownych, często nieodwracalnych szkód. Rozważmy koszt włamania za jeden grosz. Historia mówi, że w pewnym banku system internetowy został przejęty, a jeden grosz został usunięty z konta. Zobaczmy, ile ten grosz będzie kosztował bank. Po odkryciu włamania dotyczącego konta zwołano nadzwyczajne spotkanie dwudziestu dyrektorów, które trwało cztery godziny. Podjęto decyzję o uzgodnieniu wszystkich 250 000 kont banku na podstawie danych z poprzedniego dnia. Działanie to wymagałoby dwóch pełnych dni od pięcioosobowego działu IT banku. Kampania public relations została autoryzowana przez kilka mediów, aby, miejmy nadzieję, zrównoważyć wszelką negatywną reklamę. Niewątpliwie koszt włamania za jeden grosz skończył się znacznie bardziej niż strata za jeden grosz. Operacje organizacyjne nie są już fizycznie wykonywane i monitorowane, ale są wykonywane elektronicznie za pośrednictwem współużytkowanych baz danych oraz intranetów, ekstranetów i Internetu. Oznacza to, że działamy w oparciu o postrzeganie rzeczywistości, a nie z samą rzeczywistością. Menedżer banku patrzy na ekran, aby zobaczyć sytuację finansową banku, i nie liczy rachunków ani monet znajdujących się w setkach lokalizacji banku. Podczas gdy wygoda, wydajność i skuteczność zapewniane przez systemy informacyjne mają niespotykaną dotąd skalę, podobnie są związane z tym zagrożenia. W związku z tym konieczne jest, aby środki bezpieczeństwa organizacji były dostosowane do stale rosnących zagrożeń. W przypadku naruszenia bezpieczeństwa w systemie informatycznym najważniejszym środkiem bezpieczeństwa jest wykrywanie w czasie rzeczywistym, powiadamianie i natychmiastowe przeciwdziałanie. Pewna biała księga stwierdza: „Firma… musi natychmiast wykryć ataki lub słabe punkty i zapewnić skuteczne rozwiązania". Dlatego wykrywanie incydentów jest podstawą każdego planu bezpieczeństwa - planu, który jest wspierany przez zaprojektowanie bezpiecznego systemu, który zapewnia analizę incydentów i procedurę naprawy podatności.

Typowe luki w zabezpieczeniach organizacyjnych

W definicji organizacyjnego systemu informacyjnego każde wymaganie funkcjonalne musi mieć towarzyszący komponent bezpieczeństwa, reagujący zarówno na ataki zewnętrzne, jak i wewnętrzne. Według statystyk najskuteczniejsze są cyberataki natury hybrydowej. Znawca podatności, znający lukę, pomaga osobie z zewnątrz skutecznie ominąć zabezpieczenia systemu i uzyskać do niej dostęp do zasobów organizacji. Przy projektowaniu i wdrażaniu systemu informatycznego, oprócz oczekiwanej nominalnej wydajności, należy dodać funkcje bezpieczeństwa, które zapobiegną tworzeniu luk w zabezpieczeniach. Większość luk w zabezpieczeniach wynika z jednego lub więcej z poniższych:

* Kopia zapasowa danych: Tworzenie kopii zapasowych danych w odstępach niezgodnych z szybkością działania systemu. Decyzja CIO, czy kopia zapasowa danych ma być wykonywana co godzinę, minutę, sekundę czy milisekundę. Częstotliwość przenoszenia danych z miękkiego magazynu kopii zapasowych na twardy nośnik archiwalny musi być starannie dobrana. Ponadto należy podjąć decyzję co do trwałości danych i ich zasad dostępu. Usunięcie niepotrzebnych danych może być bardzo ważne, ponieważ może podlegać przepisom dotyczącym zgodności. Zależność analiz po wprowadzeniu od

danych z kopii zapasowej jest absolutna, ponieważ ścieżka dostępu do zarchiwizowanych danych może dostarczyć cennych informacji.

* Operacyjne przepełnienie bufora: każdy element wprowadzania danych lub żądania wejścia są tymczasowo przechowywane w buforze podczas obsługi. Łatwe projektowanie oprogramowania wymaga bufora o stałym rozmiarze o szacowanym rozmiarze. Bez względu na rozmiar bufor może się zapełnić, powodując, że dana funkcja nie będzie działać lub będzie niedostępna. Securityminded design software wymaga dynamicznego bufora rozmiaru, który może bez końca rozszerzać się na ogromną dostępną pamięć dyskową. Atakujący przepełniają docelowe bufory, co zwykle powoduje nadpisanie danych lub kodu. Możliwe jest, że atakujący zainstalują złośliwe oprogramowanie, które naiwny bufor może przekazać kodowi wykonywalnemu o katastrofalnych skutkach.

* Nasycenie prędkości operacyjnej: niekończące się i trwałe żądania, choć proste, może przekraczać granice obliczeniowe systemu i praktycznie uniemożliwiać komunikację zewnętrzną z użytkownikami działającymi w dobrej wierze. Ponownie, zorientowane na bezpieczeństwo projektowanie oprogramowania wymaga przepisów, aby ignorować lub blokować trwałe żądania wspólnego pochodzenia.

Autoryzacja i uwierzytelnianie dostępu

Kody i procesy autoryzacji są często wrażliwe z różnych powodów. Najczęstsze to:

• System pozwala użytkownikowi na niekończące się próby wprowadzenia hasła. W takim przypadku atakujący automatyzuje atak, używając generatora haseł, który z czasem wykrywa prawidłowe hasło.

• System nie zezwala użytkownikowi na wiele prób wprowadzenia hasła, a użytkownik zapisuje hasło w miejscach potencjalnie wrażliwych.

• System wymaga zmiany hasła w częstych odstępach czasu, powodując niedogodności dla użytkownika, a użytkownik wprowadza minimalne zmiany, a każda zmiana dodaje luki.

Obecne technologie uwierzytelniania obejmują następujące cztery czynniki:

• Coś, co użytkownik wie (np. hasło, PIN)

• Coś, co użytkownik ma (np. karta bankomatowa, karta inteligentna, urządzenie USB)

• Coś, co użytkownik (np. cecha biometryczna, np. odcisk palca)

• Coś, co użytkownik otrzymuje, np. hasła jednorazowe (OTP) otrzymane przez telefonię komórkową (takie jak usługa krótkich wiadomości, SMS) lub przez Internet (np. e-mail lub inna osobiście dostępna aplikacja)

„Nazwy użytkowników i hasła nie zapewniają już odpowiedniego bezpieczeństwa".

Udanym rozwiązaniem problemu z hasłem było użycie protokołu OTP, w którym serwer autoryzacji za pośrednictwem alternatywnego kanału wysyła do użytkownika kod OTP za każdym razem, gdy użytkownik potrzebuje dostępu do systemu. Takie hasła mogą być ważne przez krótki okres czasu, jeśli to możliwe alternatywne kanały to ;

• Telefonia komórkowa, w której serwer autoryzacji wysyła OTP na telefon komórkowy użytkownika za pomocą SMS-a, a nawet wypowiada się maszynowo

• Internet, w którym serwer autoryzacji wysyła OTP do użytkownika za pośrednictwem czatu, Skype, MSN lub e-maila

To rozwiązanie należy do kategorii tzw. uwierzytelniania dwuskładnikowego (TFA). TFA oznacza zastosowanie dwóch trybów zezwoleń , aby jak najlepiej uwierzytelnić użytkownika. Pierwszy czynnik jest umowny , taki jak nazwa użytkownika i hasło, a drugim czynnikiem jest tryb niekonwencjonalny, taki jak odpowiedź na określone pytanie lub parametr biometryczny lub parametr parabiometryczny „Dwuskładnikowe rozwiązanie uwierzytelniające wykorzystuje codzienne narzędzie - telefon [komórkowy] [który jest bardzo blisko osoby], aby zabezpieczyć [uwierzytelnianie] logowań i transakcji na kontach". Ten rodzaj uwierzytelnienia należy do kategorii parabiometrycznej. Udział telefonu komórkowego w procesie uwierzytelniania może być tak prosty, jak otrzymanie OTP lub nawet odebranie określonego hasła do uwierzytelnienia drukowania głosowego. Ponadto, nawet jeśli atakujący wprowadzi prawidłową nazwę użytkownika i hasło, autoryzowany użytkownik otrzyma natychmiastowe połączenie z informacją o dostępie. Jeśli dostęp jest próbą włamania, legalny użytkownik „może natychmiast zablokować konto i powiadomić dział oszustwa firmy, [który] może natychmiast podjąć odpowiednie działania". Procedury uwierzytelniania wieloskładnikowego (wielomodowego) są coraz częstsze i są stopniowo wdrażane w aplikacjach o wysokim poziomie bezpieczeństwa. OTP można połączyć z biometrią, gdzie odczyt odcisku palca i OTP są wysyłane do serwera w celu uzyskania dostępu do zasobów.

Czynniki ludzkie

Niesklasyfikowany raport rządu USA ujawnił, że „znaczna większość przeszłych naruszeń dotyczyła osób z zewnątrz, osób posiadających upoważnienie, które mogą ominąć fizyczną barierę bezpieczeństwa, a nie osób postronnych włamujących się do bezpiecznych obszarów". Personel, którego działalność obejmuje Internet lub inne sposoby przetwarzania danych, stanowi krytyczny zasób organizacyjny, który może przekształcić się w słaby link. Ich działalność może polegać na pisaniu kodu, programowaniu baz danych, korzystaniu z urządzenia pamięci USB lub po prostu wysyłaniu wiadomości e-mail. Każda taka czynność musi być wykonywana w określony sposób i zgodnie z polityką. „Sama technologia nie jest odpowiedzią". Ustanowienie, a także egzekwowanie zasad dotyczących wprowadzania, modyfikacji, odczytu lub usuwania danych organizacyjnych stanowi podstawę bezpieczeństwa danych w każdym przedsiębiorstwie. Równie ważna jest funkcja kontroli końcowej w systemie informatycznym, dzięki której zmiany danych można prześledzić według ich pochodzenia. Istnieje wiele sposobów powiadamiania właścicieli danych o dostępie do ich danych. W zależności od krytyczności danych można podjąć odpowiednie środki, od otrzymania wiadomości e-mail po otrzymanie wiadomości SMS na telefon komórkowy. Chociaż technologia może w rozsądny sposób chronić elektroniczne zasoby organizacji, nie może z taką samą łatwością chronić przed zagrożeniami z zewnątrz. Przytłaczające statystyki wskazują, że większość ataków na bazy danych ma charakter wewnętrzny lub zewnętrzny z pomocą wewnętrzną. Wyrażenie brzmi: nie możesz chronić się przed ochroniarzem, kucharzem lub lekarzem. Trudno jest ustalić bariery między danymi organizacyjnymi a tymi, którzy mają bona fide, muszą z nich korzystać. Organizacja nie może również traktować swoich członków jako potencjalnych przestępców. Konieczne są jednak mechanizmy bezpieczeństwa, aby żaden członek organizacji nie mógł samodzielnie spowodować poważnych szkód. Równie ważne jest to, że żaden członek organizacji nie może wpływać na dostęp do danych lub zmiany bez pozostawiania śladu. Studia przypadków i badania ankietowe wskazują, że istnieje podgrupa specjalistów w dziedzinie technologii informatycznych, którzy są szczególnie podatni na stres emocjonalny, rozczarowanie, niezadowolenie i wynikające z tego błędy w ocenie, co może prowadzić do zwiększonego ryzyka szkodliwych działań lub podatności na rekrutację lub manipulację. W ten sam sposób, w jaki poziom podatności jest przypisywany oprogramowaniu, procesom lub procedurom, powinien być również przypisywany personelowi obsługującemu krytyczne dane organizacyjne. Jest to bardzo delikatna kwestia, która, jeśli nie zostanie podana z najwyższym profesjonalizmem, może doprowadzić do powstania wyobcowania w organizacji. Dyrektor ds. Informatyki wraz z szefem działu

HR są odpowiedzialni za ocenę obecności i poziomu potencjalnej podatności na zagrożenia u każdego członka organizacji, który obsługuje krytyczne dane. W związku z tym wszyscy członkowie organizacji muszą przejść specjalne szkolenie i wytyczne dotyczące bezpieczeństwa. W przypadku sektora federalnego National Institute for Standards and Technology (NIST) dostarcza wyraźny dokument. Wytyczne są przeznaczone dla agencji rządowych, ale w równym stopniu dotyczą sektora cywilnego, kładąc nacisk na świadomość potencjalnych negatywnych konsekwencji w przypadku kompromisu w zakresie bezpieczeństwa informacji.

Służby Bezpieczeństwa

Usługi bezpieczeństwa mogą być świadczone przez wewnętrzne talenty, zewnętrzne organizacje zajmujące się bezpieczeństwem danych lub ich połączenie. Tak czy inaczej, wewnętrzny dyrektor ds. Bezpieczeństwa informacji (CISO lub CSO) jest ostatecznie odpowiedzialną osobą i najwyższym organem w zakresie definiowania, projektowania i wdrażania systemu informacyjnego, a także w późniejszych operacjach i zarządzaniu bezpieczeństwem. Znaczne korzyści można uzyskać dzięki wykorzystaniu zewnętrznych organizacji bezpieczeństwa posiadających doświadczenie i wiedzę, które przewyższają talent wewnętrzny. Zasadniczo podatność organizacyjna wzrośnie jednak, gdy zewnętrzni konsultanci ds. Bezpieczeństwa wejdą do organizacji.

Technologie zewnętrzne

Koncepcja architektury informacji przedsiębiorstwa często wykracza poza dane, bazy danych, intranet i cyberprzestrzeń i obejmuje zewnętrzne technologie i zasoby. Jednym z takich przypadków jest wykorzystanie globalnego systemu pozycjonowania (GPS) oferowanego i obsługiwanego przez Departament Obrony USA. GPS, dwadzieścia cztery systemy satelitarne, zapewnia informacje o lokalizacji w postaci długości i szerokości geograficznej, wysokości, kierunku i czasu. Rysunek pokazuje GPS i jego dwadzieścia cztery konstelacje satelitarne.

Technologia ta znajduje zastosowanie w wielu branżach, „takich jak usługi reagowania kryzysowego, egzekwowanie prawa, ochrona ładunków, transport materiałów jądrowych, nawigacja lotnicza oraz standardy czasu krytycznego i synchronizacji dla mediów, telekomunikacji i sieci komputerowych ”. Chociaż system jest bardzo dokładny, niezawodny i wolny od luk w zabezpieczeniach, „sygnały GPS nie są bezpieczne”. Odbiór radiowy dostarczonych danych może być zakłócany przez atakujących, a co gorsza, może zostać sfałszowany, sfabrykowany w celu wprowadzenia użytkownika w błąd. Dlatego błędne dane wprowadzą użytkownika w błąd co do dokładnej lokalizacji śledzonego zasobu. Na szczęście istnieją pewne środki zaradcze, które chociaż nie przywracają prawidłowych sygnałów, wskazują na błąd. W przypadku zakłócania sygnału odbiornik GPS odbiera stosunkowo silny sygnał radiowy, ale nie wytwarza danych, co prowadzi do wniosku, że sygnał jest zakłócany. Jeśli chodzi o fałszowanie, dane potwierdzone przez odebrane sygnały można potwierdzić konwencjonalnymi

środkami, na przykład weryfikując kierunek podróży za pomocą kompasu lub porównując otrzymany czas za pomocą zegara. Również sfałszowany sygnał będzie silniejszy niż oczekiwany, „1×10^{-16} watów"]. Dlatego, chociaż sygnały GPS pochodzą z bardzo wiarygodnego źródła, świadomość możliwego włamania powinna być uwzględniona w równaniu bezpieczeństwa danych organizacji.

Luki w zabezpieczeniach sieci

Sieci są najbardziej wrażliwym i krytycznym elementem w każdej organizacji i właśnie tam musimy skutecznie zapobiegać, wykrywać i reagować na zdarzenia związane z bezpieczeństwem. Cyberobrona sieci wymaga skoordynowanego zaangażowania kompleksowego portfolio narzędzi bezpieczeństwa, które dobrze ze sobą współpracują w sposób inteligentny i zautomatyzowany sposób. Nie tak dawno temu wszystkie dane organizacji, mimo że były połączone w sieć, znajdowały się w fizycznych granicach organizacji. Obecnie dostępność opłacalnego zewnętrznego przechowywania danych za pośrednictwem dostawców usługi Storage-as-a-Service (SaaS), zwanej powszechnie chmurą, stworzyła nowe luki w zabezpieczeniach. Takie opcje przechowywania danych to najlepsze z nieznanych środków bezpieczeństwa. Oznacza to, że wszelkie dane przechowywane przez organizację, przynajmniej poza jej absolutnym nadzorem, muszą być niezawodnie szyfrowane. Trendem zewnętrznego wsparcia IT, który osiągnął już poziom dostępności, jest infrastruktura jako usługa (IaaS). Oznacza to, że organizacja potrzebuje tylko komputerów z przeglądarkami internetowymi i dostępem do sieci. Niewątpliwie IaaS może zapewnić ogromne korzyści ekonomiczne organizacji, ale poziom podatności na zagrożenia jest nieznany. Sieci są głównym punktem wejścia dla cyberprzestępców, dlatego w punktach cyberprzestrzeni organizacji należy zastosować maksymalną ochronę. Praktyka polegała na stosowaniu narzędzi i technik w celu zatrzymania takich prób włamań. Takie próby muszą zostać rozpoznane i zablokowane. W tym celu dostępne są narzędzia komercyjne, określane jako Network Intrusion Prevention Systems (NIPS lub IPS), zwykle instalowane w punkcie wejścia do organizacji. NIPS służy jako cyber-policjant przy wjeździe i wyjeździe, badający każdy pakiet danych wchodzących lub wychodzących z sieci organizacji i decyduje, na podstawie zasad, czy zablokować, czy pozwolić na przejście do pakietów. Oprogramowanie IPS może odgrywać aktywną rolę, jak opisano powyżej, lub rolę pasywną, rejestrując jedynie aktywność punktu wejścia-wyjścia i opracowując statystyki, które mogą być analizowane i mogą tworzyć inteligencję.

Sieci bezprzewodowe

Sieć organizacyjna i związane z nią zasoby są również zagrożone przez luki w wewnętrznej lub zewnętrznej komunikacji bezprzewodowej. Chociaż trzy znormalizowane technologie bezprzewodowe - Bluetooth, Wi-Fi i WiMAX - mają funkcje bezpiecznej komunikacji, istnieją luki w zabezpieczeniach, które muszą być znane i odpowiednio usuwane przez użytkowników. Dzięki temu, że są bezprzewodowe i działają w zakresie częstotliwości radiowych (RF), takie sieci są narażone na niektóre zagrożenia, przed którymi trudno się obronić. To są:

• Podsłuchiwanie. Dostępność analizatorów ruchu umożliwia bardzo łatwe odbieranie i przechwytywanie wymienianych danych. Następnie dane, mimo że są zaszyfrowane, mogą być gromadzone i ewentualnie odszyfrowane w późniejszym czasie.

• Wstrzykiwanie szumu. Jest to przerywany zastrzyk impulsów szumowych RF mających na celu uszkodzenie normalnej komunikacji.

• Zagłuszanie. Potężne źródło RF nadające w pobliżu jednostek organizacji i w spektrum operacji może obezwładnić sieć. Oczywiście lokalizację źródła można łatwo zidentyfikować, chyba że źródło jest mobilne.

• man-in-the-middle. Jest to przypadek, w którym przeciwnik o podobnej łączności bezprzewodowej udaje legalną stację bazową, stację mobilną lub stację abonencką.

Najczęściej używane standardowe sieci bezprzewodowe to Bluetooth (BT), Wireless Fidelity (Wi-Fi) oraz Worldwide Interoperability Microwave Access (WiMAX).

Bluetooth

Bluetooth (BT) to nazwa handlowa transmisji danych, protokołu certyfikowanego przez IEEE (Institute of Electrical and Electronics) znany jako IEEE 802.15.1–1 Mb / s

Protokół WPAN (Wireless Personal Area Network)

Protokół którego celem jest zapewnienie „standardów łączności bezprzewodowej o niskim stopniu złożoności i niskim zużyciu energii". Pomimo obszernych środków bezpieczeństwa, które zostały wprowadzone w specyfikacjach BT, wydaje się, że konstrukcja systemu operacyjnego BT nieumyślnie pozostawiła kilka luk w zabezpieczeniach. Jednak fakt, że większość kodu BT znajduje się w oprogramowaniu wewnętrznym, sprawia, że technologia bezprzewodowa BT jest odporna na „złośliwy kod". Rysunek ilustruje BT WPAN, który służy jako zamiennik kabla o zasięgu do 30 stóp, 10 metrów.

Aby być narażonym na ryzyko włamania, urządzenie mobilne lub komputer osobisty wyposażone w BT musi mieć włączoną funkcję BT. Oznacza to, że urządzenie musi znajdować się w trybie wykrywalnym. Ponadto we wszystkich komunikatach BT - działających w dobrej wierze lub złośliwych - ofiary i atakujący urządzenia - muszą znajdować się w odległości 10 metrów od siebie, aby komunikacja mogła się odbyć. Jednak dostępność bardzo wrażliwych odbiorników umożliwia podsłuch BT z znacznie większych odległości. Luki w zabezpieczeniach urządzeń wyposażonych w BT można uznać za pasywne lub aktywne. W pasywnych intruzi szpiegują lub stwarzają niedogodności, podczas gdy w aktywnych intruzi powodują straty w bazach danych urządzeń ofiary.

Luki w zabezpieczeniach pasywnych

Obecność docelowego urządzenia można rozpoznać po pingowaniu. Powtarzające się pingowanie może renderować funkcje BT ofiary ,że urządzenie nie działa. Podczas gdy urządzenie wyposażone w BT komunikuje się, intruz może określić adres urządzenia i użyć go do komunikacji z nim, uniemożliwiając w ten sposób prawidłowe komunikowanie się z innymi urządzeniami. Ulepszenia specyfikacji BT ostatecznie wyeliminowałyby penetrację urządzeń w trybie nieodkrytym.

Bezprzewodowa technologia BT działa w nielicencjonowanym paśmie, gdzie wiele innych aplikacji uważa za równie wygodne w obsłudze. Dostępna jest technologia bezprzewodowej sieci LAN Wi-Fi, wykorzystująca to samo pasmo, podobnie jak kuchenki mikrofalowe i wiele telefonów bezprzewodowych. w związku z tym urządzenia wyposażone w BT znajdujące się w obszarze promieniowania jednego z takich produktów mogą być niezamierzone

Aktywne podatności

Za pośrednictwem komunikacji BT intruz może przejąć pełną kontrolę nad poleceniami urządzenia-ofiary - mianowicie Poleceniami AT, które sterują telefonem komórkowym - w żaden sposób nie przyciągając uwagi właściciela urządzenia-ofiary. W tej luce intruz może korzystać z urządzenia ofiary tak, jakby znajdowało się w zasięgu ręki. Dane mogą być zmieniane, połączenia i wiadomości mogą być wysyłane i odbierane, dostęp do Internetu, a nawet rozmowy mogą być słuchane przez telefon intruza Dzięki specjalnemu oprogramowaniu intruz może nie tylko uzyskać dostęp do wszystkich danych w urządzeniu ofiary, ale także może nawet odczytać unikalną identyfikację sprzętową telefonu, tzw. International Mobile Equipment Identity (IMEI)

Środki ostrożności

W specyfikacjach protokołu BT osadzono różne mechanizmy bezpieczeństwa. Jednak oprócz ustanowienia zasad bezpieczeństwa , przedsiębiorstwa mogą również wdrażać oprogramowanie BT, które skanuje środowisko i monitoruje pasmo BT

• Zidentyfikuj różne typy aktywnych urządzeń BT

• Podaj wszystkie możliwe do odzyskania atrybuty zidentyfikowanych urządzeń (klasa, nazwa i producent)

• Podaj informacje o połączeniu (parowanie)

• Zidentyfikuj dostępne usługi (faks, drukarka)

Poziom ryzyka związanego z użyciem technologii bezprzewodowej BT jest bezpośrednio związany bardziej z konkretną aplikacją, a mniej z nieodłączną architekturą BT. Biorąc pod uwagę liczne ograniczenia, na podstawie których działa technologia BT - niska moc RF, odległość, szerokość pasma - żadna wysoce wrażliwa lub krytyczna aplikacja nie zwróci się do BT o wsparcie. W zakresie tego, co oferuje, a mianowicie wymiany kabli i tak długo, jak przestrzegane są podstawowe środki ostrożności, bezprzewodowa technologia BT będzie tak bezpieczna, jak powinna być, a mianowicie w przypadku aplikacji wewnątrz biura o minimalnym bezpieczeństwie.

Wireless Fidelity

Wireless Fidelity (Wi-Fi) to nazwa handlowa protokołu transmisji danych certyfikowanego przez IEEE, technicznie zwanego IEEE 802.11 — Multi-Rate DSSS. Wi-Fi to bezprzewodowy odpowiednik przewodowego protokołu Ethernet IEEE 802.3

Główni programiści i firmy OEM utworzyły Wireless Ethernet Compatibility Alliance (WECA), aby wspierać certyfikację sprzętu Wi-Fi. WECA została założona przez branżową sieć gigantów i mikroprocesorów, w tym 3Com, Cisco, Sony, Intel, Motorola, Nokia i Toshiba, i obecnie działa jako izba rozliczeniowa urządzeń Wi-Fi z obecnym członkostwem ponad 250 producentów . Protokół 802.11 zapewnia uniwersalny standard infrastruktury bezprzewodowej sieci LAN (WLAN), dzięki któremu zagwarantowana jest interoperacyjność między „certyfikowanymi produktami Wi-Fi". Przed ustanowieniem standardu WLAN i przez dziesięciolecia aplikacje WLAN ulegały stagnacji, ponieważ

każdy z głównych producentów telekomunikacyjnych miał własne projekty. Wraz z ustanowieniem standardu Wi-Fi sieci WLAN stały się standardowym urządzeniem intranetowym. Funkcje zabezpieczeń Wi-Fi zostały pierwotnie ustanowione przez WEP, a następnie WPA i są obecnie zdefiniowane przez WPA2, a ochrona dostępu nowej generacji objęta jest standardem 802.11w. Istnieją obecnie trzy wersje standardu Wi-Fi, a mianowicie 802.11a, 802.11b i 802.11g. Wersje „a" i „g" oferują szybkość przesyłania danych 54 Mb / s, wykorzystując odpowiednio pasmo 5 GHz i 2,4 GHz. Wersja „b", najstarszy standard, ma przepływność 11 Mb / s pracującą w paśmie 2,4 GHz. nie posiadając licencji, pasmo 5,0 GHz jest bardzo zajęte. Jednak zastosowanie standardu 802.11h, który obsługuje dynamiczny wybór częstotliwości i kontrolę mocy transmisji, zapewnia „współistnienie Wi-Fi z innymi typami urządzeń częstotliwości radiowych", takich jak BT. Następna wersja Wi-Fi to 802.11n. Standard „n" nie tylko czterokrotnie zwiększa przepływ danych, osiągając zakres 200–600 Mb / s, ale jest również wstecznie kompatybilny ze starszymi wersjami „a", „b" i „g". Wersja „n" korzysta z dostępności wystarczającej przepustowości, a „dzięki wielu antenom [i] bardziej inteligentnemu kodowaniu ... [dąży] do uzyskania surowych prędkości transmisji danych do 600 Mb / s". W bezprzewodowym systemie Wi-Fi, z wyjątkiem oprogramowania, istnieją dwa fizyczne komponenty: punkt dostępowy (AP) i moduł interfejsu bezprzewodowego, który jest kartą wkładaną, układem wbudowanym lub urządzeniem USB. Centralnym elementem systemu jest punkt dostępowy, który łączy świat „bezprzewodowy" z przewodowym, zwanym infrastrukturą. Zatem AP z jednej strony komunikuje się z siecią organizacji, tzw. Infrastrukturą, a z drugiej strony komunikuje się z klientami bezprzewodowymi i służy jako router spełniający potrzeby sieciowe stacji bezprzewodowych. AP zapewnia wspólny dostęp do sieci LAN / Internet za pomocą translacji adresów sieciowych (NAT). W niechronionym środowisku Wi-Fi strażnik (WD) może wykorzystać przepustowość ofiary, aby uzyskać dostęp do wszystkiego, co jest dostępne. WD może co najmniej uzyskać dostęp do Internetu lub intranetu ofiary, a maksymalnie WD może uzyskać dostęp do wszystkich plików na komputerze ofiary i przeniknąć do dowolnego innego miejsca, które jest dostępne dla komputera ofiary. Innymi słowy, w niezabezpieczonym środowisku Wi-Fi, WD może przejąć pełną kontrolę nad komputerem ofiary. Warto wspomnieć, że każda wizyta WD w Internecie będzie oznaczać tożsamość routera ofiary, co może sugerować, że ofiara nie jest łatwym dowodem na przejęcie Wi-Fi. W mediach pojawiło się wiele przypadków porwania Wi-Fi, które są zbyt smutne, by o nich wspominać. Poniżej znajduje się lista środków ostrożności, których należy przestrzegać podczas korzystania z Wi-Fi w środowisku domowym.

* Jeden: Wyłącz tryb IBSS. W tym trybie jednostka mobilna jest otwarta na komunikację bez żadnych ograniczeń. Hakerzy mogą łączyć i dyskretnie uzyskiwać dostęp do poufnych informacji. Takie ryzyko można wyeliminować, jeśli IBSS zostanie wyłączony. Wyłącz także połączenie Wi-Fi, gdy tylko nie będzie już potrzebne.

* Dwa: Wyłącz tryb infrastruktury. Tryb infrastruktury umożliwia klientom Wi-Fi dostęp do zasobów po drugiej stronie punktu dostępu (drukarki, serwery itp.).

* Trzy: Wyłącz nadawanie SSID. Ponieważ w środowisku domowym nie przewiduje się nieoczekiwanych urządzeń Wi-Fi, punkt dostępu nie musi transmitować swojej tożsamości SSID na cały świat. Zwykle ten identyfikator jest wprowadzany ręcznie i tylko raz podczas logowania do laptopa, a następnie zapamiętywany

* Cztery: Zmień dostęp routera. Router, znajdujący się w punkcie dostępowym, jest dostępny poprzez nazwę i hasło. Są one ustawiane przy pierwszej instalacji, ale można je ponownie skonfigurować w dowolnym momencie. Te dwa parametry należy zmieniać w odstępach czasu. Ponadto domyślny fikcyjny lokalny, intranetowy adres IP, który mógł mieć postać 192.168.1.1, można zmienić na dowolny inny, o ile liczby w czterech polach mieszczą się w zakresie od 0 do 224, bez zer wiodących. Ponadto „nie ma potrzeby zachowania domyślnej nazwy routera". Przeciwnie, każda zmiana w stosunku do

wartości domyślnych przyczyni się do poprawy bezpieczeństwa. Zazwyczaj wartości domyślne są takie same dla wszystkich punktów dostępu danego producenta i są zwykle znane intruzom.

* Pięć: Włącz szyfrowanie. Specyfikacja Wi-Fi obejmuje tak zwaną ochronę przewodową (WEP). Algorytm szyfrowania występuje w 40 i 64 bitach. Późniejsza wersja, WPA2, ma 128 bitów. Za każdym razem, gdy jednostka mobilna loguje się do punktu dostępowego Wi-Fi, nazwa użytkownika i hasło mogą być łatwo przechwycone przez „sniffera". Jednym ze sposobów, aby temu zapobiec, jest użycie PKI, gdzie każda strona zna klucz publiczny drugiej strony i „klucz dostępu" można ustanowić w ramach szyfrowania bez ujawniania żadnych niezaszyfrowanych informacji. Najnowsza wersja protokołu bezpieczeństwa Wi-Fi, WPA2, zapewnia PKI. Należy zauważyć, że szyfrowanie rozpuszcza się, gdy dane dotrą do miejsca docelowego. Oznacza to, że WPA2 służy wyłącznie do transportu powietrznego. Ponadto „podstawowy algorytm [szyfrowania] jest wadliwy i podlega stosunkowo łatwemu łamaniu." Istnieją nawet strony internetowe, które zapewniają kroki do złamania WEP.

* Sześć: Włącz filtrowanie adresów MAC. Zwykle punkty dostępu Wi-Fi zawierają bramę z funkcją filtrowania Media Access Control (MAC). Można zezwolić filtrowi na przekazywanie ruchu tylko z urządzeń o znanych adresach MAC. Urządzenia te mogą znajdować się w infrastrukturze (tzn. Po przewodowej stronie punktu dostępu), mogą być drukarkami lub innymi komputerami lub mogą znajdować się w przestrzeni bezprzewodowej - na karcie Wi-Fi laptopa, Wi- Fi PDA i tym podobne. W sieci bezprzewodowej znany jest identyfikator SSID, a następnie „bez filtrowania adresu MAC, każdy klient bezprzewodowy może dołączyć ". Nie powstrzyma to jednak zaawansowanego hakera, który wie, jak przechwytywać pakiety i wyciągać z nich adresy SSID i MAC.

* Soedem: Zbadaj fale radiowe. Korzystając ze specjalistycznego oprogramowania, takiego jak darmowy sniffer pakietów Ethereal, trzeba często szukać fal radiowych w poszukiwaniu nieoczekiwanych punktów dostępu Wi-Fi lub klientów Wi-Fi. Takie narzędzia, jak Ethereal, mogą przechwytywać dane „bezpośrednio z połączeń sieciowych na żywo ... mogą odczytywać przechwycone pliki ... rozpakowywać je w locie… [i mogą obecnie analizować] ... 759 protokołów"

Środki ostrożności dotyczące Wi-Fi w hotspocie

Dla wygody klientów publiczne hotspoty nie używają żadnej z możliwych funkcji bezpieczeństwa Wi-Fi (szyfrowanie WEP lub WPA) lub sieci (filtrowanie MAC). Aby ułatwić połączenia klientów, punkty dostępu Wi-Fi faktycznie nadają swój identyfikator SSID. W hotspocie klienci zaczynają od włączenia opcji Wi-Fi, połączenia z punktem dostępu, przesłania prawidłowego numeru karty kredytowej i połączenie zostaje nawiązane. Aby jednostka mobilna mogła komunikować się z punktem dostępowym, znajomość identyfikatora SSID punktu dostępu jest konieczny. Aby włamać się do klienta Wi-Fi, jednostka mobilna nie musi komunikować się z żadnym punktem dostępu. Sam fakt włączenia funkcji Wi-Fi jest wystarczający do ustalenia podatności. Klienci Wi-Fi w publicznych lub korporacyjnych hotspotach muszą podjąć szereg środków ostrożności, aby zmaksymalizować ochronę swoich poufnych informacji przed intruzami. Poniżej znajduje się kilka środków ostrożności, które należy podjąć podczas pobytu w hotspocie.

* Jeden: Hotspot Legitimacy. Hakerzy często tworzą fałszywy punkt dostępu w pobliżu legalnego publicznego punktu dostępu i próbują zwabić osoby poszukujące połączenia. Dzięki takim połączeniom hakerzy przechwytują poufne informacje (nazwy użytkowników, hasła, numery kart kredytowych itp.), Dokonując później nielegalnego wykorzystania. Klienci Wi-Fi muszą absolutnie upewnić się, że hotspot, z którym próbują się połączyć, jest uzasadniony. Zazwyczaj w obiekcie powiązanym z usługą hotspot (poczekalnie, kawiarnie itp.) umieszczane są odpowiednie znaki. Istnieje kilka stron internetowych, które wymieniają znane legalne hotspoty na całym świecie.

* Dwa: szyfrowanie plików. Pliki, w tym wiadomości e-mail, powinny zostać zaszyfrowane przed przesłaniem. Istnieje wiele opcji szyfrowania przy użyciu dedykowanego oprogramowania lub funkcji wbudowanych w aplikacje, takie jak edytory tekstu i klienci poczty e-mail. Można zainstalować aplikację szyfrującą, która „automatycznie szyfruje cały ... przychodzący i wychodzący ruch internetowy".

* Trzy: udostępnianie plików. Będąc w punkcie aktywnym, wyłącz opcję udostępniania plików, aby zapobiec niepożądanemu transferowi plików.

* Cztery: Włącz VPN . W ten sposób przechwycone dane są renderowane i bezużyteczne z powodu szyfrowania.

* Pięć: użycie zapory. Hotspot najprawdopodobniej używa jednego statycznego adresu IP do obsługi 200 klientów. Oznacza to, że wszyscy klienci znajdują się w tej samej podsieci, co ułatwia intruzowi-klientowi węszenie na innych klientach. Problem ten można zminimalizować za pomocą „osobistej zapory ogniowej". Można kupić zaporę ogniową lub skorzystać z zapory dostarczonej przez system Windows. Za pośrednictwem zapory można ograniczyć ruch i zablokować lub zezwolić na „komunikację, która może… być niebezpieczna".

* Sześć: praktyczne zasady. Niezależnie od tego, czy ktoś ma dostęp do zewnętrznego świata przewodowo lub bezprzewodowo, obowiązują również pewne dodatkowe środki ostrożności: korzystanie z najnowszego oprogramowania antywirusowego, korzystanie z najnowszej wersji systemu operacyjnego, korzystanie z bezpiecznej poczty e-mail opartej na Internecie (https), indywidualna ochrona hasłem dla poufnych pliki, a także mechanizm haseł komputerowych, który blokuje komputer, jeśli przez X minut nie ma aktywności klawiatury ani myszy

Środki ostrożności dotyczące Wi-Fi w przedsiębiorstwie

Korporacyjne zabezpieczenia Wi-Fi wymagają znacznie poważniejszego wyeliminowania luk w Wi-Fi. W takich przypadkach zaawansowane protokoły i sieci VPN są w porządku. W środowisku korporacyjnym bezpieczeństwo Wi-Fi i środki ostrożności mogą obejmować wszystkie wyżej opisane, a także te poniżej.

* Jeden: ogrodzenie obwodowe. Obecnie dostępne są rozwiązania, w których pozycjonowanie czujników RF może geometrycznie określić, czy klient znajduje się w autoryzowanym obszarze fizycznym. Takie technologie, które wymagają szkolenia w terenie i dokładnego dostrojenia, zapewniają 100% bezpieczeństwa podczas testów. Za pomocą ogrodzenia obwodowego „Środowiska Wi-Fi można chronić w przestrzeni powietrznej 3D [z dokładnością] ... około 5 stóp".

* Dwa: zaawansowane uwierzytelnianie. Zamiast polegać na nominalnych funkcjach bezpieczeństwa Wi-Fi, przedsiębiorstwo może korzystać z zaawansowanych protokołów autoryzacji / uwierzytelniania, takich jak DIAMETER.

Wi-Fi stało się obecnie podstawową technologią w lokalnej komunikacji bezprzewodowej. Jego główne luki w zabezpieczeniach - przechwytywanie sesji, man-in-the-middle i denial-of-service - są stale ograniczane poprzez postępy w technologiach bezpieczeństwa i zwiększoną świadomość bezpieczeństwa po stronie użytkowników. Wraz ze wzrostem efektywnej prędkości transmisji danych przekraczającej 200 Mb / s, będzie dużo przepustowości dla zaawansowanych technik szyfrowania i zaawansowanych protokołów autoryzacji / uwierzytelniania. Oczekuje się, że standard bezpieczeństwa 802.11w, z kluczem szyfrowania dla pakietu i dodatkowymi zaawansowanymi funkcjami, znacznie zwiększy bezpieczeństwo Wi-Fi i zmniejszy liczbę udanych ataków intruzów

Dostęp do mikrofali na całym świecie

Ogólnoświatowy interoperacyjny dostęp mikrofalowy (WiMAX) to IEEE Wireless Networking Standard 802.16, który został wydany w 2004 roku. Jego specyfikacje są stale ulepszane, wprowadzając poprawki mające na celu uczynienie z niego realnej bezprzewodowej wymiany technologii kablowej, ADSL i T1 . WiMAX działający jako stacjonarna lub mobilna sieć LAN lub Metropolitan Area Networks (MAN) wykorzystuje licencjonowane i nielicencjonowane pasma częstotliwości odpowiednio dla transmisji o wysokiej i niskiej mocy, aby zapewnić Broadband Wireless Access (BWA).

Funkcje WiMAX

Nielicencjonowane pasma w widmie 2–10 GHz ograniczają zasięg do zasięgu Wi-Fi, który wynosi około 10 do 50 metrów, a moc nadawania jest zwykle ograniczona do 200 mW. Licencjonowane pasma w zakresie widzenia w linii 10–66 GHz, w których transmitowana moc może osiągnąć 20 watów, mogą oferować zasięg w promieniu 50 km od pojedynczej stacji bazowej. Ponadto standardowa szybkość transmisji danych WiMAX wynosi 70 Mb / s. Kilku sprzedawców laptopów oferuje jednostki „gotowe do WiMAX", dostępne są również adaptery USB WiMAX. Technologia WiMAX jest również wykorzystywana do połączeń na duże odległości punkt-punkt za pośrednictwem repeaterów za pomocą anten kierunkowych. Funkcje WiMAX obejmują

• Roaming - zapewnia mobilność klienta (802.16e)

• Forward error error - wykorzystuje algorytmy tolerancji błędów

• Modulacja adaptacyjna - zmienia zakres przepustowości

• Uwierzytelnianie użytkownika i urządzenia

• Poufność przesyłanych wiadomości danych

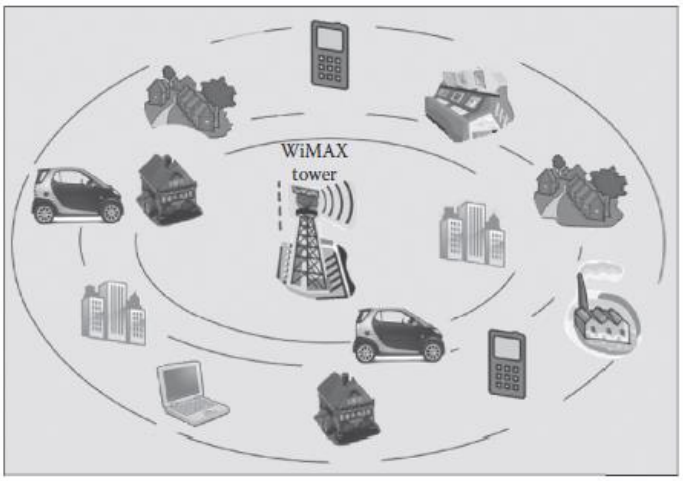
• Wysoka przepustowość danych - osiąga 75 Mb / s

• Szyfrowanie Triple-DES - do uwierzytelniania i transmisji

• AAS — wykorzystuje zaawansowane techniki antenowe (802.16e)

• Prędkość do 1 Gb / s i 100 Mb / s odpowiednio dla operacji stacjonarnych i mobilnych (802.16m)

Rysunek 2.9 ilustruje możliwe środowisko WiMAX, w którym Internet jest świadczony w promieniu 50 km dla całej populacji.



W tym scenariuszu Internet jest zapewniany jednemu użytkownikowi za pomocą telefonu komórkowego, laptopa lub komputera stacjonarnego, a także organizacjom wielu użytkowników, takim jak budynki biurowe, budynki mieszkalne lub parki przemysłowe. W przeciwieństwie do dostawców produktów i usług WiMAX badacze twierdzą, że istnieje kilka luk w technologii WiMAX. Po wprowadzeniu specyfikacji 802.16e większość domniemanych luk została usunięta. Pozostają jednak następujące luki, jak wskazano w raporcie NIST.

• Kompleksowe bezpieczeństwo (tj. urządzenie z urządzeniem) nie jest możliwe bez zastosowania dodatkowych środków kontroli bezpieczeństwa, które nie są określone w standardach IEEE.

• Dane SA (Security Associations) nie mogą być stosowane do wiadomości zarządzania, które nigdy nie są szyfrowane.

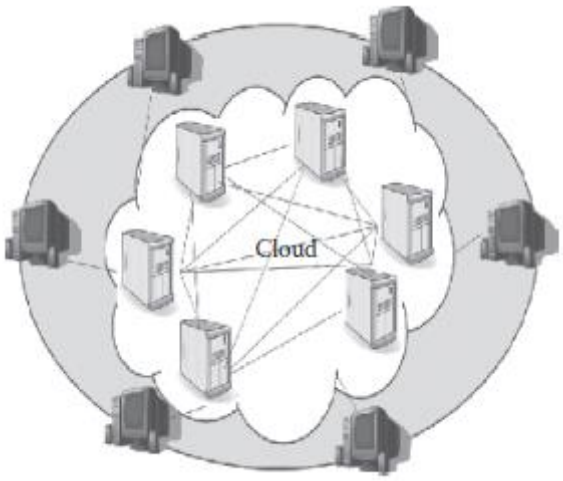
• Brak wzajemnego uwierzytelnienia może pozwolić podstępnej BS (stacji bazowej) na podszywanie się pod legalną BS, przez co SS / MS (stacja abonencka / stacja mobilna) nie będzie w stanie zweryfikować autentyczności wiadomości protokołu odebranych od BS.

Dlatego w celu zachowania poufności komunikatów zarządzania użytkownicy WiMAX muszą udoskonalić swój własny system bezpieczeństwa. W takim przypadku można również użyć standardowej umowy Diffie – Hellmana, która jest często stosowana w przypadkach, gdy poufna komunikacja musi rozpocząć się bez uprzedniej wymiany kluczy. Lista środków zaradczych, które mogą zmniejszyć ryzyko w sieciach bezprzewodowych, jest opisana w dokumentach przygotowanych przez NIST

Chmura obliczeniowa

Skutkiem tego jest coraz niższy koszt sprzętu komputerowego i telekomunikacyjnego w połączeniu ze standaryzacją oprogramowania.

Chmura obliczeniowa. Termin „przetwarzanie w chmurze” odnosi się do nowej koncepcji pozyskiwania mocy obliczeniowej jako usługi. Ta usługa jest świadczona z połączonych zasobów, w których użytkownik nie ma wiedzy o fizycznym pochodzeniu takiej usługi. Rysunek ilustruje koncepcję przetwarzania w chmurze, w której użytkownicy potrzebują tylko dostępu do Internetu.



Dostawcy takich usług mogą nawet współdzielić zasoby, tworząc usługę, która może być równoległa do dystrybucji energii elektrycznej. W tym kontekście moc obliczeniowa obejmuje oprogramowanie, sprzęt wirtualny, przechowywanie danych i dostęp do danych. W pewnym sensie jest podobny do

koncepcji dzielenie czasu w latach siedemdziesiątych, ale jest ono znacznie bardziej wydajne i dostępne za pośrednictwem Internetu, a nie modemów telefonicznych. Obecnie w przypadku przetwarzania w chmurze organizacja nie potrzebuje centrum komputerowego, ponieważ wszystkie potrzeby obliczeniowe są realizowane i świadczone jako usługa przez Internet. Przetwarzanie w chmurze należy do czterech podstawowych definicji.

Chmura publiczna: komercyjne centrum ogromnych zasobów obliczeniowych, które są udostępniane społeczeństwu na żądanie w sposób dozowany.

Prywatna chmura: prywatne centrum współdzielonych zasobów obliczeniowych, które są dostarczane członkom społeczności na żądanie w sposób dozowany. Środki bezpieczeństwa i prywatności są dostosowane do potrzeb właścicieli.

Chmura społecznościowa: będące własnością społeczności centrum ogromnych zasobów obliczeniowych, które są dostarczane członkom społeczności na żądanie w sposób dozowany. Środki bezpieczeństwa i prywatności są dostosowane do potrzeb społeczności.

Chmura hybrydowa: połączenie powyższych opcji

Dostawcy usług przetwarzania w chmurze oferują infrastrukturę, platformę i oprogramowanie jako usługę (odpowiednio w skrócie IaaS, PaaS i SaaS). Użytkownicy subskrybują takie usługi i konfigurują własne wirtualne centrum komputerowe z serwerami i bazami danych, tak jakby kupowali sprzęt fizyczny w tym celu. W takim trybie operacyjnym organizacja może w dowolnym momencie zmienić konfigurację i skalować potrzeby obliczeniowe i być obciążana opłatami według zużycia. Motto tej nowej branży brzmi: „kup dokładnie taką pojemność, jakiej potrzebujesz, kiedy jej potrzebujesz, na godzinę lub w ramach abonamentu miesięcznego. Aplikacje i dane użytkowników dostarczane przez współdzielone centra danych mogą znajdować się w zróżnicowanych geograficznie lokalizacjach, a nawet mogą zmieniać lokalizacje w sposób przejrzysty dla użytkownika. Jednak wszystko jest dostępne w Internecie za pośrednictwem tych samych adresów logicznych. Dzięki udostępnianiu ekranu, a także udostępnianiu aplikacji w chmurze, przetwarzanie w chmurze stało się jeszcze bardziej atrakcyjne dla interakcji przez Internet. Przetwarzanie w chmurze zyskuje coraz większe wsparcie jako praktyczne rozwiązanie do budowy korporacyjnego centrum danych w sposób zwirtualizowany i bez alokacji fizycznej przestrzeni. Poniżej mamy listę najbardziej uznanych zalet przetwarzania w chmurze.

1. Rekonfiguracja Użytkownicy mogą przeprojektować swoją infrastrukturę obliczeniową jednym kliknięciem myszy, wybierając i usuwając zasoby (serwery, pamięć masową, aplikacje, sieci i usługi) w zależności od potrzeb.

2. Obsługa interfejsu API Interfejs programowania aplikacji jest możliwy do interakcji oprogramowania w chmurze z maszynami lub ludźmi.

3. Niższe koszty Przetwarzanie w chmurze zmniejsza bariery wejścia na rynek, ułatwiając tworzenie centrów danych organizacji z odmierzonych zasobów za pomocą modelu biznesowego „na żądanie”.

4. Ograniczone umiejętności Niezbędne umiejętności konfigurowania i utrzymywania zwirtualizowanego centrum danych w chmurze są znacznie mniej wymagające niż umiejętności utrzymania centrum fizycznego.

5. Łączność Usługi łączności w chmurze obejmują dostęp do Internetu oraz telefon komórkowy.

6. Niezawodność Korzystanie z wielu zbędnych witryn może zapewnić ciągłość biznesową i odzyskiwanie po awarii.

7. Skalowalność Przetwarzanie w chmurze zapewnia skalowalność na żądanie w trybie samoobsługowym, umożliwiając rekonfigurację systemu w celu zwiększenia lub zmniejszenia wielkości lub zużycia zasobów.

8. Bezpieczeństwo Zapewnione są funkcje bezpieczeństwa, które zwykle są zbyt drogie, na które stać poszczególnych użytkowników.

9. Konserwacja Dostawcy usług przetwarzania w chmurze

Nie ma wątpliwości, że przetwarzanie w chmurze jest bardzo silnym nieodwracalnym trendem, ale wraz z nim pojawiają się wyzwania związane z bezpieczeństwem i prywatnością, które przekładają się na podatności na zagrożenia, które należy dokładnie rozważyć przed wejściem do tego ogrodu różanego. „Wyzwania związane z bezpieczeństwem przetwarzania w chmurze są jednak ogromne, szczególnie w przypadku chmur publicznych, których infrastruktura i zasoby obliczeniowe są własnością podmiotu zewnętrznego, który sprzedaje te usługi ogółowi społeczeństwa". Powyższe oświadczenie, pochodzące od bardzo autorytatywnego organu, takiego jak NIST, może sprawić, że CIO i CSO zatrzymają się. Istnieje silna obawa, że powierzona opieka powierzona fizycznemu przechowywaniu wrażliwych danych organizacyjnych stanowi sama w sobie poważną lukę. Dla wielu i z definicji przetwarzanie w chmurze jest niezabezpieczonym środowiskiem. Jednak dla rosnącej liczby, przetwarzanie w chmurze jest właściwą drogą i pozostanie. Jeśli chodzi o bezpieczeństwo i prywatność, można podjąć dodatkowe środki w celu dostosowania tego nowego trybu do tradycyjnych wewnętrznych centrów danych w tym zakresie. Przed przystąpieniem do przejścia na przetwarzanie w chmurze należy uzyskać weryfikowalne gwarancje, że wymogi bezpieczeństwa i prywatności w organizacji są w pełni spełnione. Dostawcy usług w chmurze często oferują umowy usługowe, które nie podlegają negocjacji. Nie jest to jednak absolutne i można je wynegocjować. Należy podkreślić, że system przetwarzania w chmurze obejmuje oprogramowanie klienckie oraz jego oprogramowanie i urządzenia dostępowe, a także po tej stronie należy zabezpieczyć zasady bezpieczeństwa i prywatności. W razie potrzeby dostawca usług przetwarzania w chmurze powinien być w stanie wykazać skuteczność oferowanych usług, zwłaszcza tych związanych z bezpieczeństwem i prywatnością. Często kontrolerzy zewnętrzni są przyprowadzani w celu potwierdzenia ważności żądanych usług. Przetwarzanie w chmurze należy do ogólnej kategorii outsourcingu, ze wszystkimi związanymi z tym zagrożeniami. Dlatego przed przystąpieniem do takich umów wymagana jest dokładna analiza ryzyka. Główne dostrzegane wady subskrypcji środowiska przetwarzania w chmurze wymieniono poniżej.

• Złożoność systemu	• Z powodu platform chmurowych, zwłaszcza publicznych ich rozmiar i zwiększona funkcjonalność są otwarte na błędy i podatności.
• Wiele dzierżawców	• Obawy dotyczą środowiska współdzielonego przez wielu dzierżawców zasoby, brak silnego podziału na kategorie może skutkować problemy z bezpieczeństwem lub prywatnością.
• Internet vs.intranet	• Przetwarzanie w chmurze jest dostępne w Internecie i z definicji mniej bezpieczne niż izolowany intranet organizacyjny.
• Personel	• Personel chmury publicznej może nie mieć wymaganych wymagań poziom poświadczenia bezpieczeństwa.
• Forensics	• W środowisku chmurowym, w zależności od poziomu wewnętrznego w przypadku audytu może nie być możliwe powiązanie wykonanych usług powiązany sprzęt. Ponadto poprzednie ciągi komputerów i działania

generowane przez ludzi mogą być trudne do prześledzenia i udokumentowania do akceptowalnego przez sąd poziomu i może być niemożliwe do powielenia.

• Zasady chmurowe	• Zasady bezpieczeństwa i prywatności dostawców usług przetwarzania w chmurze oraz praktyki mogą, ale nie muszą być zgodne z praktykami wymagającymi prywatnych lub lokatorzy rządowi.
• Przejęcie konta	• Chociaż przykłady nie są dostępne, istnieje duże zaniepokojenie w Internecie możliwość włamania poświadczeń i późniejszej strony internetowej kompromis.
• Przerwa w świadczeniu usług	• Istnieje wiele przykładów, w których przyczyny są poza kontrolą dostawcy usług w chmurze spowodowali przerwy w pracy na kilka godzin w najmniej oczekiwane czasy. Jest to problem, który można dobrze sformułować w umowa serwisowa, ale piorun nie przeczyta jej przed uderzeniem.
• Reakcja na incydent	• Takie zdarzenie będzie wymagało skoordynowanego wysiłku służby subskrybent i usługodawca w ogromnym zadaniu audytu śledzenie, które może obejmować wcześniejsze użycie wspólnego sprzętu.

Podczas gdy „przejście do outsourcingu publicznego środowiska przetwarzania w chmurze jest pod wieloma względami ćwiczeniem w zakresie zarządzania ryzykiem", przetwarzanie w chmurze, które jest obecnie w powijakach, ostatecznie stanie się głównym hostem centrum danych ze względu na swoją opłacalność, która poprawi się w porównaniu z czasem.

Internet przedmiotów

Pierwsza era cyberprzestrzeni miała miejsce, gdy jej jedynymi mieszkańcami były komputery. Ogromnym osiągnięciem było posiadanie jednej sieci - Internetu obejmującej cały świat, a także możliwość wysyłania i odbierania tekstu, audio i wideo w czasie rzeczywistym. Druga era cyberprzestrzeni miała miejsce, gdy zalały ją smartfony, znacznie przewyższając liczbę podłączonych komputerów. Wkroczyliśmy w trzecią erę cyberprzestrzeni, w której zostanie zalana rzeczami, dzięki czemu stanie się Internetem Rzeczy (IoT). Oczekuje się, że do roku 2020 będzie 24 miliardów urządzeń IoT obsługujących świat w praktycznie każdym aspekcie życia. Wraz z napływem urządzeń IoT pojemność protokołu IPv4, który może pomieścić do $4{,}3 \times 10^9$ adresów IP, będzie wymagać uaktualnienia do protokołu Ipv6, który pomieści ponad 340×10^{36} adresów IP - astronomiczny 39- cyfra Uważa się jednak, że protokół IPv4 będzie wystarczający w najbliższej przyszłości. Są to znormalizowane urządzenia dostępne w Internecie z możliwością komunikacji z czujnikami i urządzeniami wykonawczymi, umożliwiając nam interakcję w czasie rzeczywistym w praktycznie dowolnym środowisku. W skrócie, przez Internet lub Bluetooth, urządzenia IoT bez ograniczeń wykrywają, komunikują się, analizują i działają. Urządzenia IoT mogą służyć jako autonomiczne inteligentne czynniki, usprawniające operacje w celu zwiększenia skuteczności, bezpieczeństwa i wydajności. Poziom innowacji osiągnie niespotykane wyżyny. Ogólnie oczekujemy, że zobaczymy:

- Nieograniczona i wszechobecna łączność
- Redukcja kosztów produktów i usług
- Miniaturyzacja
- Postępy w analizie danych

• Wzrost w chmurze obliczeniowej

• Zmniejszenie zużycia energii dzięki inteligentnemu sterowaniu oświetleniem i temperaturą

• Lepsza opieka zdrowotna dzięki cichemu monitorowaniu 24/7

• Zwiększa produktywność

• Nie do pomyślenia produkt i usługi

Rzeczywiście, dzięki wykorzystaniu urządzeń IoT społeczeństwo będzie czerpać znaczne korzyści. Konkretne zastosowania Internetu Rzeczy obejmują następujące przykłady:

• Śledzenie zwierząt gospodarskich, upewniając się, że każda jest odpowiednio karmiony.

• Śledzenie drzew, upewniając się, że nie ma nielegalnych działań związanych z wylesianiem.

• Wyczuwanie wilgoci w glebie w celu optymalnego nawadniania działek w miarę potrzeby.

• Wykorzystanie urządzeń monitorujących zdrowie do monitorowania wartości parametrów zdrowotnych, takich jak oddychanie, bicie serca, temperatura, ciśnienie krwi itp., Przy jednoczesnym natychmiastowym powiadamianiu o odchyleniach od oczekiwanych wartości.

• Zdalne rejestrowanie zużycia energii elektrycznej, które poprzednio wymagało od osoby odczytania każdego licznika elektrycznego w mieście, deszczu lub świecenia.

• Automatyczny wykrywacz awarii i dyspozytor pomocy awaryjnej.

• Reporter miejsca parkingowego, w którym strona internetowa wyświetla lokalizację dostępnego parkingu.

• Parametry śledzenia pojazdów flotowych, takie jak lokalizacja, prędkość, poziom paliwa, temperatura silnika itp.

Biorąc pod uwagę, że urządzenia IoT wykorzystują mikrokontrolery - komputery jednoukładowe - o ograniczonej mocy obliczeniowej i pojemności pamięci, równolegle z powyższymi oczekiwaniami budzą wiele obaw, podobnych do tych zgłaszanych podczas wprowadzania smartfonów, takich jak:

• Co stanowi dobrą praktykę projektową?

• Jaki jest poziom tolerancji na uszkodzenia?

• Czy jest nadmiarowość?

• Czy usterki są wykrywalne i usuwalne?

• Czy istnieją wystarczające zasoby edukacyjne, aby wyprodukować tak dużą liczbę inżynierów Internetu Rzeczy?

• Czy gromadzone dane są odpowiednio oznaczone datą?

• W jaki sposób monitorowana jest wydajność?

• W jaki sposób ocenia się i ocenia ryzyko bezpieczeństwa?

• W jaki sposób chroniona jest poufność danych, uwierzytelnianie i kontrola dostępu?

• W jaki sposób nastąpi modernizacja?

• Jak długo potrwa, zanim zostaną ustanowione standardy branżowe urządzeń IoT?

• Jak długo potrwa, zanim zostanie ustanowiona legalna infrastruktura IoT?

• Jak będą obsługiwane awarie bezpieczeństwa lub wydajności?

• Czy urządzenia IoT powinny mieć wymuszone wygaśnięcie, wyłączając je w określonym momencie?

Przy tak wielu oczach i uszach na całym świecie jest rzeczą naturalną, że poruszone zostaną kwestie prywatności. W wielu przypadkach będzie to niezapowiedziane naruszenie prywatności bez zgody, a nawet świadomości. Przykład podniesionych już problemów związanych z prywatnością urządzeń IoT jest następujący:

• Gromadzenie danych: tryb, wykorzystanie i usuwanie.

• Preferencje prywatności: wyrażenie, egzekwowanie, przejrzystość.

• De-personalizacja danych „statystycznych" gromadzonych za pośrednictwem urządzeń IoT.

• Równowaga między prywatnością a bezpieczeństwem.

• Prywatność od samego początku.

• Problemy z odpowiedzialnością i zaufaniem.

Prawdą jest, że jeśli czujniki są wszędzie, praca organów ścigania będzie łatwiejsza. Na przykład kamery w miejscach publicznych mogą, miejmy nadzieję, powstrzymać przestępczość, a urządzenie IoT w każdym samochodzie ułatwi odzyskanie, jeśli zostanie skradzione, ale takie aplikacje, jeśli zostaną wykorzystane, mogą spowodować poważne naruszenia wolności obywatelskich. Niezależnie od zastosowania lub potencjalnego nadużycia, urządzenia IoT powinny być tak zaprojektowane aby :

• Poziom wbudowanych zabezpieczeń jest proporcjonalny do zastosowania urządzenia.

• Choć bezpieczny, szanuje prywatność gromadzonych danych.

• Domniemana prywatność jest weryfikowalna.

• Osobiste identyfikatory są usuwalne.

• Klucze szyfrujące są bezpieczne i zarządzane.

Zgodnie z oczekiwaniami istnieje wiele przykładów problemów z bezpieczeństwem lub nadużyć w stosowaniu urządzeń IoT, przy czym bezpieczeństwo fizyczne urządzeń jest najmniejsze. Typowe przypadki to gdzie

• Jeden z głównych producentów samochodów musiał wycofać ponad milion samochodów, aby naprawić usterkę, która umożliwi ingerencję bezprzewodową w samochody.

• W kraju Europy Wschodniej cyberprzestępcy zamknęli całą sieć energetyczną, pogrążając się w ciemnościach i zimnych milionach mieszkańców.

• W innym kraju europejskim cyber-szpiedzy, z powietrza, nie chcieli wybierać kanałów telewizyjnych, aby udowodnić swoje zdolności hakerskie.

Podsumowując, niewątpliwie technologia Internetu przedmiotów jest bardzo obiecująca dla producentów urządzeń, dla przedsiębiorstw, które je zintegrują, oraz dla konsumentów, którzy będą z

nich korzystać. Przed nami jednak wyzwania, szczególnie na dwóch frontach, a mianowicie: stać się prywatnymi i bezpiecznymi oraz przekonać świat, że są prywatne i bezpieczne.

Cyberbezpieczeństwo motoryzacyjne

Cyberprzestrzeń rozwija się i obejmuje całkowicie nienaruszone dziedziny, takie jak przemysł motoryzacyjny i kierowca. To kwestia czasu, kiedy producenci samochodów będą oferować „Internet w samochodzie" jako standardową funkcję. Kierowca po prostu włoży kartę SIM telefonu komórkowego, a pojazd „zapełni" się Wi-Fi. Wi-Fi będzie dostarczane z urządzeniem Pandora oferującym niespotykane funkcje:

• Wsparcie nawigacji

• Doradztwo drogowe w czasie rzeczywistym

• Przybycie wybranego e-maila

• Wykrywanie awaryjne i wezwanie pomocy

• Raportowanie wydajności pojazdu

• Raportowanie wydajności kierowcy

• Nieograniczone opcje rozrywki

• Rozpoznawanie głosu dla tożsamości i kontroli

• Zdalny dostęp i wykrywanie

Zasadniczo komfort salonu i wydajność biura zostaną połączone w fotelu kierowcy, czyli w centrum dowodzenia i kontroli kierowcy. Wraz z bogactwem funkcji - zwiększonym bezpieczeństwem, wydajnością i rozrywką - powstaje „szeroki obszar cyberataków", ku radości hakerów i cyberprzestępców. Z definicji wszystko w sieci, przewodowo lub bezprzewodowo podlega hakowaniu. Ingerencja w lokalną sieć kontrolowanego obszaru pojazdu (CAN) może wstrzykiwać polecenia ze zdalnej lokalizacji, zdolnej do przejęcia danych i funkcji krytycznych z punktu widzenia bezpieczeństwa i innych niż bezpieczeństwo, co może mieć wpływ na zdolność kierowcy do kontrolowania pojazdu. Rządy przewidujące nadchodzącą integrację pojazdu z Internetem przygotowały szeroko zakrojone badania, wskazujące na ryzyko, które towarzyszy wraz z szybkim przyjęciem technologii. Na szczęście opracowano standardy cyberbezpieczeństwa dla „Cyber-fizycznych pojazdów samochodowych". Zdarzały się przypadki zdalnego dostępu do elementów sterujących pojazdu, które potencjalnie mogły stworzyć niebezpieczną sytuację. Podsumowując, we wszystkich sektorach cyberbezpieczeństwo pozostaje mieszanym błogosławieństwem, wymagającym dokładnych słabych punktów i oceny ryzyka. Takie badania wymagają profesjonalnej znajomości branży motoryzacyjnej, a także cyberbezpieczeństwa. W końcu każdy pojazd musi być postrzegany jako wielofunkcyjne „urządzenie" Internetu Rzeczy, które należy chronić przed możliwymi cyberprzestępstwami

Narzędzia oceny podatności

Dzisiejsze korzystanie z Internetu przypomina pływanie w wodach wypełnionych rekinami. Wirusy internetowe zwykle po cichu wykonują swoje własne zadania kopiowania lub niszczenia plików lub instalowania kodu, który spowoduje jeszcze więcej szkód. Często aktywne wirusy spowalniają komputer lub działają dziwnie.

Na szczęście dostępnych jest wiele narzędzi antywirusowych, które mogą zminimalizować takie ryzyko, jeśli nie wyeliminować je. Należy podkreślić, że ciągłe infekowanie Internetu nowymi i potężniejszymi

wirusami uniemożliwia absolutne poleganie na narzędziach antywirusowych. Zazwyczaj działania wykonywane przez takie narzędzia antywirusowe obejmują:

• Zbieranie adresów IP ruchu przychodzącego i wychodzącego

• Śledzenie zgodności użytkownika z zasadami organizacji

• Wykrywanie wzorców ataku

• Wykrywanie nietypowych działań użytkownika

• Ocena integralności transferów plików

• Analizy zebranych danych pod kątem kryteriów bezpieczeństwa cybernetycznego

Jednak zainstalowanie bieżącego narzędzia antywirusowego w systemie jest rozsądne i utrzymanie go w trybie automatycznym jest koniecznością. W przypadku braku trybu automatycznego codzienne skanowanie jest niezbędne.