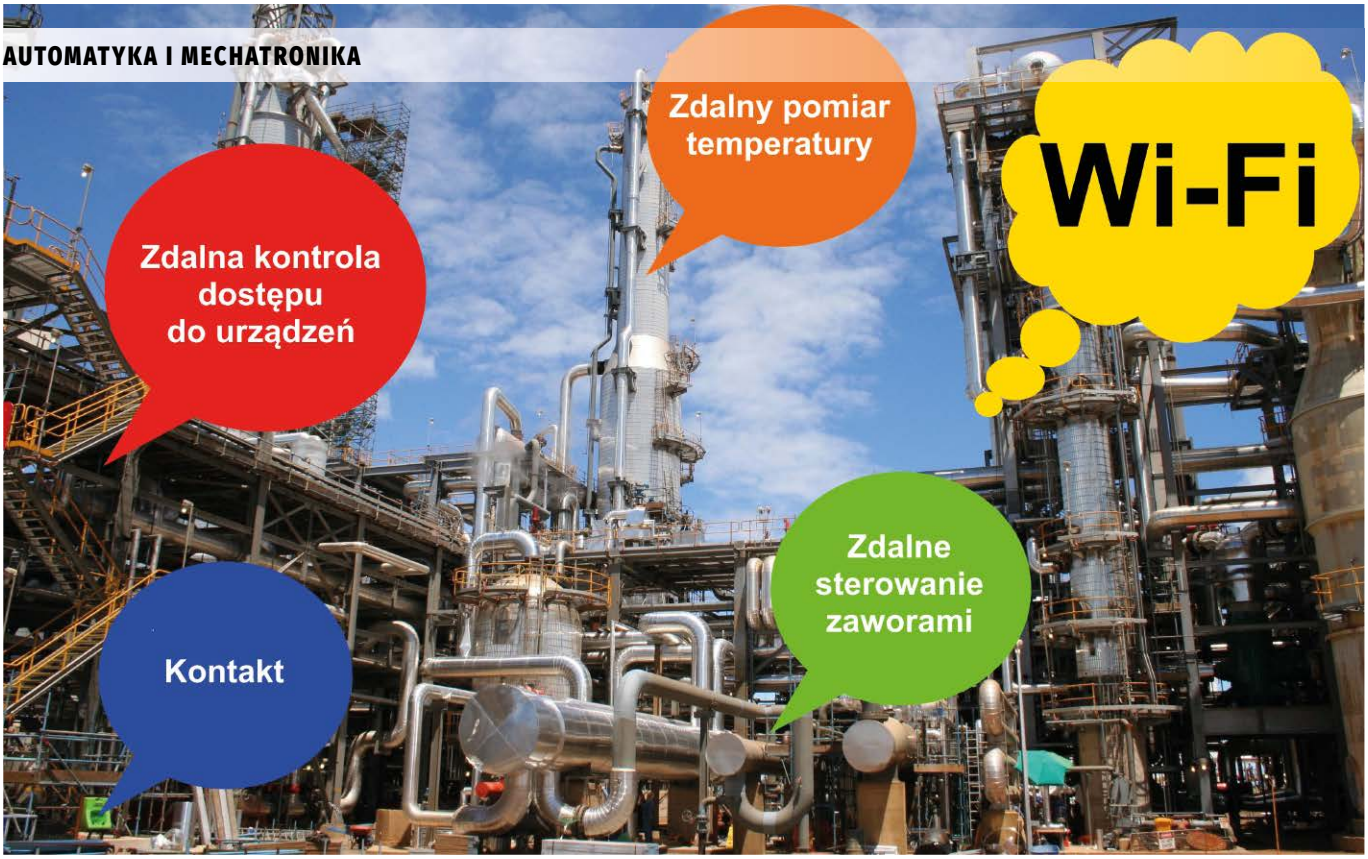

Sieć Wi-Fi w przemyśle

Udogodnienia i zagrożenia

Współcześnie sieci bezprzewodowe są niemal wszędzie. Przeciętny użytkownik najlepiej zna je z zastosowań domowych, ale upowszechniły się one również w zakładach przemysłowych. Brak konieczności prowadzenia kabli połączeniowych, dostępność sieci w niemal dowolnej lokalizacji i szeroka znajomość posługiwania się tym rodzajem łączności są powodami, dla których stosowanie Wi-Fi jest bardzo wygodne, ale czy bezpieczne w tak odpowiedzialnych zastosowaniach?

Łączność Wi-Fi jest powszechnie używana, jednak jak każda technologia wymaga zrozumienia zasady jej działania, zwłaszcza w zastosowaniach wymagających podwyższonego poziomu bezpieczeństwa, do których zaliczyłbym m.in. sieci przemysłowe. Niestety, wydaje się, że niewiele osób rozumie zasady bezpiecznej komunikacji, a jeszcze mniej poziom bezpieczeństwa zapewnianego przez różne rodzaje zabezpieczeń – metody kodowania transmisji.

Standard Wi-Fi służy do tworzenia lokalnych, bezprzewodowych sieci cyfrowych. Sposób transmisji został opisany w standardzie IEE802.11, opublikowanym przez organizację IEEE w 1999 r. Tak naprawdę, w tamtym czasie był to jedyny, praktyczny mechanizm łączności bezprzewodowej, mający (jak na tamte czasy) stosunkowo dużą prędkość transmisji danych (do 2 Mb/s). Standard bardzo szybko upowszechnił się, a rosnące wymagania użytkowników spowodowały jego dalszy rozwój. We współczesnych zastosowaniach, przy bardzo dobrej jakości sygnału i użyciu popularnych, dostępnych urządzeń jest możliwe osiągnięcie prędkości nawet 300 Mb/s. Trzeba mieć jednak świadomość, że dołączanie kolejnych urządzeń do sieci spowalnia transmisję, ponieważ kanał radiowy jest współdzielony.

W tamtych latach, gdy wprowadzano Wi-Fi, królowały sieci ArcNet pracujące w topologii ring, w których okablowanie prowadzono za pomocą przewodu koncentrycznego. W przemyśle stosowano interfejsy szeregowe RS232/RS485 o „zawrotnej prędkości" np. 9600 b/s. Brak było też wspólnego, standardowego rozwiązania zapewniającego integralność przesyłanych danych, co zmuszało producentów sprzętu do opracowywania własnych protokołów komunikacyjnych. Była to, co prawda, sytuacja wygodna dla wytwórców urządzeń, którzy mogli oferować unikatowe rozwiązania skazując klientów na użytkowanie produktów pochodzących wyłącznie od danego producenta, ale doprowadziła do sytuacji, w której na rynku urządzeń przemysłowych panował ogromny bałagan. Nie pasowały złącza, protokoły, w wielu wypadkach nie można było łączyć ze sobą urządzeń różnych producentów. Trudno dziwić się, że w takiej sytuacji wszyscy dosłownie „rzucili się" na nowy standard, który dawał szansę na uporządkowanie sytuacji.

W zastosowaniach przemysłowych technologia Wi-Fi utworzyła możliwości do wdrażania komunikacji o dużej prędkości (w porównaniu do interfejsów szeregowych), ponieważ urządzenia końcowe nadal wykorzystywały protokoły szeregowe. Komunikacja przebiegała w topologii punkt-punkt przy użyciu jednostki RTU (Remote Terminal Unit) z protokołem np. Modbus. Bezpieczeństwo takich połączeń nie było problemem, ponieważ gdyby ktoś nieupoważniony zdołał „włamać" się do tej transmisji, to ewentualne szkody miały niewielki zasięg, a włamywacz nie miał dostępu do innych danych przedsiębiorstwa. Chcąc zdezorganizować pracę fabryki taki włamywacz również nie miałby zbyt wielu możliwości – jedynie wpływ na pojedynczą maszynę lub sterownik, z którym był połączony. Jednak ze względu na stosowanie różnych standardów przez różnych producentów (urządzenia RTU zwykle pełniły też rolę translatorów protokołów komunikacyjnych) możliwość wpływu na tak połączone urządzenia również nie byłaby zbyt wielka.

W miarę upływu lat różne technologie IT były coraz liczniej adoptowane przez przemysł, a sieci Ethernet – przewodowe i bezprzewodowe – wkroczyły do hal fabrycznych. Sieci te wykorzystujące protokoły TCP/IP i UDP zaczęły być normą w przedsiębiorstwach, ale obok nich nadal używano firmowych protokołów przemysłowych, takich jak Modbus TCP/IP, Profinet, EtherNet/IP oraz innych. Jednocześnie sieci, do których były włączone urządzenia przemysłowe zaczęły być dołączane do komputerów biurowych, co z jednej strony usprawniło pracę przedsiębiorstwa, ale z drugiej spowodowało też liczne, nowe zagrożenia. Sieci przemysłowe stawały się coraz bardziej podobne do typowych sieci domowych lub biurowych. Jednocześnie sieci przemysłowe, które były w naturalny sposób były odizolowane stały się dostępne. Każdy użytkownik sieci biurowej mógł połączyć się z dowolnym urządzeniem przemysłowym. Od tego momentu dostęp do danych i potencjalna możliwość ich kradzieży stały się łatwiejsze, ponieważ potencjalny włamywacz mógł skorzystać z metod, których nauczył się korzystając ze sprzętu dostępnego w domu lub w biurze.

Mimo tego, iż w sieciach przemysłowych nadal było mało danych stanowiących atrakcję dla włamywacza, to ci szybko odkryli, że w wielu przedsiębiorstwach połączenia pomiędzy urządzeniami są słabo zabezpieczone (bo po co ktoś miałby się tam włamywać?), a jednocześnie istnieje możliwość sięgnięcia za ich pomocą o sieci biurowej przedsiębiorstwa. Hakerzy zaczęli więc wykorzystywać te same kanały komunikacyjne, które utworzono dla kadry zarządzającej, a służące do przesyłania danych dotyczących produkcji do oprogramowania korporacyjnego – zwykle takie włamanie nie wymagało dużego wysiłku.

W takiej sytuacji w przedsiębiorstwach zaczęto coraz powszechniej instalować urządzenia umożliwiające dostęp bezprzewodowy Wi-Fi. Zwykle były to rutery lub punkty dostępowe mające za zadanie doraźne rozwiązanie problemu połączenie punkt-punkt w sytuacjach, gdy nie było możliwe ułożenie kabli. Już w tych wczesnych urządzeniach sieciowych implementowano zabezpieczenia komunikacji, jednak ze względu na wygodę użytkowników oraz wiarę w to, że „i tak nikt się nie włamie" nie korzystano z nich pozostawiając łącza niezabezpieczone. Przed 2003 r. dostępną w sieciach Wi-Fi metodą szyfrowania połączeń był WEP opisany w ogólnych zaleceniach standardu, ale dedykowany rynkom konsumenckim, a nie zastosowaniom wymagającym podwyższonego poziomu bezpieczeństwa. Jak pokazało życie, kodowanie WEP było słabym zabezpieczeniem, łatwym do złamania. W latach 2003-2006 obowiązywał standard WPA z algorytmem szyfrującym TKIP lub AES. Standard ten okazał się lepszy, ale również stosunkowo szybko poddał się zabiegom hakerów. Współcześnie stosuje się WPA2 ze 128-bitowym lub dłuższym blokiem danych szyfrowanym za pomocą algorytmu AES i z protokołem CCMP. Jest on stosunkowo trudny do złamania, ale nie jest to niemożliwe. Wymaga jednak to od potencjalnego hakera sporo czasu i wysiłku włożonego w złamanie zabezpieczeń, więc – ze względu na małą atrakcyjność danych – przeważnie jest po prostu niewarte wysiłku.

Wprowadzenie zabezpieczenia AES+CCMP co prawda rozwiązało problem włamań, ale tylko teoretycznie. W związku z tym, że czas funkcjonowania urządzeń przemysłowych zwykle jest dosyć długi, to nowe urządzenia dostępowe musiały zapewniać kompatybilność wsteczną, aby użytkownik mógł również skonfigurować połączenia ze starszymi urządzeniami. Zwykle bardzo dobrej jakości przemysłowe urządzenia dostępowe mogą pracować przez wiele lat, ponieważ nie jest wymagana duża prędkość transmisji pomiędzy komputerami w przedsiębiorstwie a typowo pracującą bardzo wolno

maszyną. W wielu przedsiębiorstwach nietrudno znaleźć sprzęt zainstalowany przed rokiem 2003 r., kiedy to było dostępne tylko zabezpieczenie WEP. Wiele osób będących instalatorami tego typu sprzętu to służby utrzymania ruchu, a nie personel IT. Z kolei, użytkownikowi maszyny jest wszystko jedno, jaki standard transmisji jest stosowany do transmisji danych – byle nie powodował przestojów i awarii sprzętu. Personel utrzymania ruchu często montuje nowy router w miejsce starego i nie rozumiejąc zabezpieczeń konfiguruje go dla zachowania kompatybilności do pracy z zabezpieczeniem WEP. Bo przecież po włączeniu szyfrowania WEP teoretycznie połączenie jest zabezpieczone, więc „zrobiliśmy swoje, jesteśmy kryci". Mało tego, niektóre połączenia sieciowe nawet nie są instalowane przez pracowników firmy, bo na przykład programiści maszyn lub serwisanci będący pracownikami firm zewnętrznych mogą dla wygody podłączyć router bezprzewodowy lub punkt dostępowy do sterownika PLC lub sieci firmowej. Często robią to w dobrej wierze, aby pomóc w rozwiązaniu pewnych problemów. W wielu firmach takie działania są zabronione, ale serwisant może coś zrobić po kryjomu, pomimo tego. Poza tym, jeśli kultura zabezpieczeń nie jest w danym przedsiębiorstwie na zbyt wysokim poziomie, to takie praktyki mogą być na porządku dziennym.

Jeśli potencjalny włamywacz korzystając z ogólnie dostępnych narzędzi skanujących sieci odkryje taką lukę, to sieć jest praktycznie bezbronna przed jego działaniami. Otwiera to potencjalną możliwość włamania się do sieci informatycznej przedsiębiorstwa, co może mieć opłakane konsekwencje.

Jak przeciwdziałać takim sytuacjom? Po pierwsze, należy ograniczyć możliwość fizycznego dostępu do sieci radiowej. Haker mający zamiar włamać się do sieci korporacyjnej zwykle idzie po najmniejszej linii oporu szukając niezabezpieczonej lub niewystarczająco zabezpieczonej sieci bezprzewodowej. Głównym utrudnieniem w takiej sytuacji będzie dla niego brak możliwości zbliżenia się do hali fabrycznej lub budynku biurowca na odległość skutecznego zasięgu sieci Wi-Fi. Niestety, większość urządzeń jest wyposażonych w anteny dookólne i emituje wystarczająco silny sygnał, o zasięgu przekraczającym ogrodzenie przedsiębiorstwa. Dla hakera, który może w takiej sytuacji posłużyć się dodatkowym sprzętem poprawiającym zasięg, w większości wypadków nawiązanie połączenia z siecią Wi-Fi nie stanowi problemu, ale instalując urządzenia trzeba mieć na uwadze to zalecenie ograniczając, jeśli to możliwe, emisję sygnału radiowego do użytecznej odległości..

Od strony warstwy fizycznej warto zrobić przegląd urządzeń pracujących w przedsiębiorstwie i wymienić starsze punkty dostępowe lub rutery, wyprodukowane przez 2006 r. na nowsze, obsługujące szyfrowanie WPA2. W takiej sytuacji będzie można skonfigurować zabezpieczenia wszystkich połączeń za pomocą standardu WPA2 i szyfrowania AES+CCMP. Warto też używać tzw. silnych haseł, które są trudne do odtworzenia i przy tym niekoniecznie trudne do zapamiętania. Użytkownicy mogą używać fraz zawierających łatwe do skojarzenia wyrazy, liczby i znaki. Na przykład „WizytaWLondynieMarzec2016". Do wygenerowania unikatowych haseł można też użyć specjalnych programów. Należy też stworzyć system zarządzania hasłami, aby mieć pewność, że wszystkie są bezpieczne. Trzeba też zwracać uwagę na personel, ponieważ nawet najlepszy system zarządzania hasłami jest bezsilny wobec… karteczek naklejonych na urządzenie. System zarządzania hasłami powinien też uwzględniać sytuację, w której pracownik mający wiedzę na temat urządzeń i ich konfiguracji rozstaje się z firmą. Znanych jest wiele przypadków, w których niezadowolony, były pracownik szkodzi zakładowi korzystając ze swojej wiedzy. Jest on o wiele bardziej niebezpieczny od hakera, ponieważ dysponuje gruntowną wiedzą na temat przedsiębiorstwa. W najgorszej sytuacji, doświadczony pracownik może podzielić się swoją wiedzą ze zdolnym hakerem. Dlatego powinna być możliwa natychmiastowa lub niemal natychmiastowa zmiana loginów i haseł. Zaleca się też, aby wszystkie hasła były zanotowane na papierze i przechowywane w bezpiecznym miejscu, poza przedsiębiorstwem. Na wszelki wypadek powinno one być dostępne również w firmie – na przykład, w bezpiecznym segregatorze przechowywanym w sejfie.

Od strony zabezpieczeń IT warto ograniczyć możliwość łączenia się z siecią korporacyjną za pomocą Wi-Fi. Jeśli potencjalny włamywacz może połączyć się bezprzewodowo z ruterem w przedsiębiorstwie, to należy maksymalnie ograniczyć ilość możliwych szkód, które może wyrządzić. Włamanie do przemysłowej sieci Wi-Fi nie może torować hakerowi drogi do zasobów przedsiębiorstwa, w których przechowuje się najbardziej wartościowe, poufne dane.

Połączenie pomiędzy siecią przemysłową a siecią biurową umożliwia sprawny przepływ danych i zarządzanie produkcją, dlatego bardzo trudno jest się go wyrzec. Trzeba jednak zastosować pewne ograniczenia, aby z jednej strony uniemożliwić nieuprawnionym pracownikom biurowym ingerencję w proces produkcji, a z drugiej zabronić dostępu hakerom, którzy mogą dostać się do sieci korporacyjnej poprzez sieć przemysłową. Może to jednak kłócić się z praktyką stosowaną w niektórych zakładach produkcyjnych, które albo chcą, albo potrzebują komunikacji „w obu kierunkach" w celu wysyłania instrukcji produkcyjnych lub pobierania danych o bieżących procesach produkcyjnych.

Aby zabezpieczyć się przed nieautoryzowanym dostępem, personel IT w przedsiębiorstwach instaluje specjalne firewalle pomiędzy sieciami biurowymi a przemysłowymi. W takiej sytuacji komunikacja pomiędzy obiema sieciami odbywa się za pomocą stref DMZ lub specjalnych serwerów, co umożliwia kontrolowanie przepływu danych. Jednak wykorzystując tę personel IT strategię zwykle koncentruje się on na kontrolowaniu danych „spływających" na produkcję, zaniedbując ruch w odwrotnym kierunku. Ponadto, zdarza się, że osoby dbające o oprogramowanie korporacyjne nie mają wystarczającej wiedzy na temat sieci przemysłowych i sprzęcie sieciowym używanym na produkcji i dlatego reguły ruchu rzadko są konfigurowane, jak powinny. Więc jeśli haker chce włamać się do sieci poprzez sieć przemysłową, to wystarczy, że dostanie się wystarczająco blisko hali fabrycznej, aby ustanowić komunikację. Jeśli uda mu się w ten sposób dostać do sieci korporacyjnej i ma odpowiednie umiejętności, to przypuszczalnie bez trudu otworzy sobie „ścieżkę" i kolejne „odwiedziny" będzie mógł odbywać niekoniecznie korzystając z sieci przemysłowej i odkrytej luki w zabezpieczeniach. Może np. „odwiedzać" przedsiębiorstwo przez Internet korzystając z faktu, że większość serwerów korporacyjnych ma takie połączenie. Jeśli tego połączenia nie ma, można je bez trudu utworzyć instalując w pobliżu fabryki ruter bezprzewodowy lub inne urządzeni dostępowe, a dane przesyłać do wygodniejszych dla siebie, nawet znacznie oddalonych lokalizacji. Dosyć jest stwierdzić, że zręczny włamywacz znajdzie wiele sposobów na utworzenie takiego linku i w ten sposób może trwale „zaczepić się" w sieci korporacyjnej chociażby z użyciem sieci telefonii komórkowej.

Jednak nie tylko sieć korporacyjna, ale również przemysłowa, jest warta zabezpieczenia. Współcześnie wiele przedsiębiorstw używa w procesie produkcji programowanych obrabiarek CNC. Kradzież danych przesyłanych do takiej maszyny może być bardzo dotkliwa zwłaszcza, jeśli dotyczy krytycznego procesu będącego tajemnicą firmy. Aby jednak skraść takie dane, trzeba dysponować odpowiednimi umiejętnościami i wiedzą, której brak przeciętnemu hakerowi. Nie licząc pojedynczych przypadków, większość włamań będzie dokonywana przez amatorów, zwykłych „szkodników", którym z jakiegoś powodu sprawia radość zakłócenie produkcji poprzez wyłączenie maszyny, usuniecie programu z pamięci sterownika lub komputera przemysłowego. Niestety, w skrajnych wypadkach trzeba też liczyć się z możliwością ataku terrorystycznego.

Jeśli system sterowania umożliwia hakerowi działania wywierające trwały wpływ na przedsiębiorstwo lub jego otoczenie, to jest po prostu źle zaprojektowany i należy poddać go ponownej ocenie, weryfikacji i zmodyfikować, jeśli to konieczne. W poprawnie zaprojektowanym systemie sterowania można wywołać pewne problemy, ale są one odwracalne, krótkotrwałe. Z drugiej strony, nie można jednak powiedzieć, że „nasza fabryka jest dobrze zabezpieczona" i zlekceważyć bezpieczeństwo sieci przemysłowej lub korporacyjnej, a w szczególności sieci bezprzewodowych.

Jest dobrą praktyką, aby plan przygotowany na wypadek ataku odzwierciedlał wartość chronionych zasobów lub procesów. Nie powinno być możliwości zakłócenia pracy prawidłowo zaprojektowanego systemu sterowania, obojętnie czy to przez błąd człowieka, czy oprogramowania. Właściwe zabezpieczenie sieci przemysłowej, zwłaszcza mającej możliwość dostępu zdalnego za pomocą Wi-Fi, wymaga systematyczności i nakładu pracy oraz dalece posuniętej ostrożności przy jej użytkowaniu. Aby jednak zapewnić właściwy poziom bezpieczeństwa, należy uczulić pracowników na kwestie związane z bezpieczeństwem sieci. Trzeba też okresowo dokonywać jej audytu, aby wykryć potencjalne luki i źródła zagrożenia.

Opisane w artykule sposoby zabezpieczenia sieci to w zasadzie podstawowe działania, których podjęcie nie wymaga wielkich nakładów finansowych. Ich wdrożenie może być ważnym aspektem działalności przedsiębiorstwa i przyczynić się do jego niezakłóconego działania.

JACEK BOGUSZ, EP