PROBLEMATYKA BEZPIECZEŃSTWA INFORMATYCZNEGO W INTELIGENTNYCH SIECIACH

Krzysztof Billewicz

Instytut Energoelektryki Politechnika Wrocławska

Obecnie coraz bardziej wady i zalety inteligentnych sieci (Smart Grid). Dodatkowo jednak pojawia się kwestia bezpieczeństwa informatycznego takich sieci. Jednym z głównych zagrożeń jest możliwość ingerencji cyberprzestępców. Zwiększanie automatyzacji i komunikacji w ramach inteligentnych sieci ma właśnie tę zła stronę: zwiększenie podatności sieci na ataki.

1. WPROWADZENIE

Można powiedzieć, że rozwój elektroenergetyki w kierunku inteligentnych sieci (smart grid) jest bardzo prawdopodobnym scenariuszem. Powszechne zastosowanie inteligentnych urządzeń oraz zaawansowanego oprogramowania znaczne ułatwi efektywne, skuteczne oraz bezpieczne zarządzanie i eksploatowanie tych sieci. Jednak inteligentna sieć oparta jest o rozwiązania informatyczne, które jednak niosą ze sobą pewne zagrożenia. Jednym z głównych zagrożeń jest możliwość ingerencji cyberprzestępców. Zapewnienie, przez lata, prawidłowego funkcjonowania takich sieci, ich bezpieczeństwa oraz ochrony przed atakami hackerów staje się poważnym problemem.

2. POLITYKA BEZPIECZEŃSTWA – TEORIA

Polityka bezpieczeństwa (ang. security policy) jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby i w jaki sposób mają być chronione [wikipedia.org]. Polityka bezpieczeństwa powinna być dokumentem spisanym, dostępnym dla pracowników. Każdy z nich po zapoznaniu się z jego treścią powinien potwierdzić ten fakt własnoręcznie złożonym podpisem.

Polityka bezpieczeństwa obejmuje swym zakresem całość zagadnień związanych z bezpieczeństwem danych, posiadanych przez przedsiębiorstwo, a nie tylko samą sieć komputerową lub dostęp do systemu informatycznego. Polityka bezpieczeństwa powinna konkretnie określać pożądane oraz niedopuszczalne zachowania związane z wykorzystaniem kont użytkowników oraz dostępnych zasobów danych. Polityka bezpieczeństwa nie jest dokumentem statycznym. Wymaga ciągłych modyfikacji dostosowujących zapisy do zmieniających się uwarunkowań pracy firmy.

Zasoby chronione to: oprogramowanie, sprzęt komputerowy, dane firmy, ludzie, dokumentacja sprzętu, oraz dane krytyczne firmy: dane o kontrahentach, informacje handlowe, dane narażające na utratę pozytywnego wizerunku, sposoby nieautoryzowanego dostępu itd.

Dodatkowo należy kierować się zasadą przydzielania najmniejszych uprawnień do aplikacji oraz do danych. Dostęp do zasobów powinien być ograniczony tylko do osób, dla które ten dostęp powinny mieć.

Należy również określić:

— poziom akceptowanego ryzyka,
— mechanizmy kontroli dostępu,
— mechanizmy identyfikacji oraz autoryzowania dostępu,
— rejestrację dokonywanych zmian w systemie: konfiguracyjnych oraz modyfikacji danych
— śledzenie zdarzeń w systemie.

Nie sposób uniknąć błędów podczas pracy z aplikacją. Pomyłki pracowników często spowodowane są niekompetencją lub przemęczeniem. Aby zminimalizować ryzyko pracownikom nadaje się minimum uprawnień oraz nie przydziela się nadmiaru obowiązków, które mogłyby przeszkodzić w przemyślanej pracy z systemem informatycznym.

3. POLITYKA BEZPIECZEŃSTWA – PRAKTYKA

Coraz ważniejszym zagadnieniem stają się weryfikacja, pewność i bezpieczeństwo danych. Aby zmniejszyć ilość danych nieprawidłowych zabezpiecza się sieci przed próbami włamania się hackerów i manipulowania przez nich danych, do których nie powinni posiadać dostępu. Mnoży się procedury polityki bezpieczeństwa, które utrudniają pracę normalnym użytkownikom aplikacji.

Każdy z użytkowników powinien mieć dostęp do aplikacji po prawidłowym zalogowaniu się. W przypadku trzeciej, nieprawidłowej próby wpisania hasła, dostęp dla tego użytkownika powinien być nieaktywny przez ok. 15 minut.

Użytkownicy aplikacji to ludzie, którzy korzystają z Internetu. Zapewne każdy z nich musi pamiętać hasła do:

— konta użytkownika podczas logowania się do komputera służbowego,
— konta użytkownika podczas logowania się do komputera prywatnego,
— aplikacji pomiarowo-rozliczeniowej,
— konta poczty służbowej,
— konta poczty prywatnej,
— portalu przedsiębiorstwa pracy,
— konta bankowego,
— PIN do karty bankomatowej,
— PIN do karty kredytowej,
— PIN do karty SIM telefonu służbowego,
— PIN do karty SIM telefonu prywatnego,
— portalu społecznościowego np. Facebook.pl, nasza-klasa.pl,
— forum, z którego korzysta,
— serwisu aukcyjnego lub zakupowego: allegro.pl, ebay.pl, snajper.pl itp.
— komunikatora internetowego np. Skype, Gadu-gadu,
— innych portali, które wymagają autoryzowanego dostępu np. portal szkolny dziennik internetowy, portale specjalistyczne itp.

Do tego polityka bezpieczeństwa niektórych zakładów pracy wymuszają okresową zmianę haseł. Nowe hasła muszą różnić się np. od 10 poprzednich, nie mogą być zbyt proste np. takie jak nazwa użytkownika. Dodatkowo muszą one zawierać małe i wielkie litery, cyfry oraz znaki dodatkowe.

Przeciętny pracownik po 5 zmianie hasła przestaje panować nad hasłami. Dlatego albo wprowadza jedno hasło, identyczne do wszystkich aplikacji, albo zapisuje je w pliku lub na łatwo dostępnej kartce papieru np. znajdującej się w podręcznej szufladzie. Czasami na monitorze przyklejona jest kartka z obecnym hasłem logowania do systemu.

Konsekwencje takiej polityki bezpieczeństwa nie są trudne do przewidzenia. Bezpieczeństwo tak chronionego systemu coraz bardziej staje się fikcją. Dlatego coraz poważniejszym zagadnieniem staje się inna, niż za pomocą haseł statycznych, autoryzacja użytkownika (ang. authorization) lub kontrola dostępu (ang. access control). Pewnym rozwiązaniem jest stosowanie tokenów lub dokonywania uwierzytelnienia na podstawie danych biometrycznych (np. odciski palców). Obecnie stosowane automatyczne podpowiadanie haseł w nowszych systemach operacyjnych powoduje, że cyberprzestępca dostając się usługą terminalową na tę maszynę można bez trudu zalogować się na konto jej użytkownika.

Pracownicy powinni zapoznać się szczegółowo z treścią Polityki bezpieczeństwa obowiązującą w przedsiębiorstwie. Jednak czasami zdarza się, że zapoznają się z tym dokumentem pobieżnie z powodu dużej liczby obowiązków, albo w krótkim czasie zapomną część przeczytanych zapisów, które powinni stosować. Takie podejście pracowników naraża przedsiębiorstwo na straty, w tym również finansowe.

Dostawca usług informatycznych w przypadku serwisowania aplikacji oczekuje dostępu do zabezpieczonych komputerów. Każde skomplikowanie dla takiego dostępu wydłuża czas wykonywania usługi serwisowej, co w przypadku niemożności realizacji kluczowych procesów biznesowych u OSD, naraża go na dodatkowe, czasem niemałe, koszty. Do tego dochodzą kwestie upgrade aplikacji, czyli podstawiania nowszych wersji programu lub takich, z poprawionymi usterkami. Każda komplikacja w kwestii dostępu do zasobów serwisowanego komputera również wydłuża czas naprawy usterki. Nieprawidłowo lub zbyt rygorystycznie stosowana polityka bezpieczeństwa utrudnia pracę z serwisowaną aplikacją oraz naraża OSD na dodatkowe koszty.

4. NAJCZĘSTSZE ZAGROŻENIA SYSTEMÓW INFORMATYCZNYCH

Do najczęstszych zagrożeń systemów informatycznych należy zaliczyć [2]:

- Zablokowanie dostępu do usługi,
- Włamanie do infrastruktury systemu informacyjnego,
- Utrata danych,
- Kradzież danych,
- Ujawnienie danych poufnych,
- Zafałszowanie informacji,
- Kradzież kodu oprogramowania,
- Kradzież sprzętu,
- Uszkodzenia systemów komputerowych.

5. BEZPIECZEŃSTWO INTELIGENTNEJ SIECI

Inteligentne Sieci mają coraz bardziej strategiczne znaczenie w kwestii bezpieczeństwa energetycznego. Inteligentna sieć jest unowocześnieniem istniejących sieci energetycznych. Umożliwia lepszą diagnostykę pracy sieci oraz pozwala sieciom podejmować działania samonaprawcze (oczywiście w określonym zakresie). Dodatkowo umożliwia dynamiczne zintegrowanie lokalnych źródeł energii, w tym również odnawialnej oraz bardziej efektywnie wykorzystywać energię elektryczną. Zwiększenie automatyzacji i komunikacji w ramach sieci elektrycznej oprócz wielu niewątpliwych zalet ma również, przynajmniej teoretycznie, ciemną stronę: zwiększenie podatności na ataki [3].

Obecnie funkcjonowanie sieci elektroenergetycznej oraz sprawna kontrola jej pracy zależy od wielu komputerów, sieci komputerowych, oprogramowania oraz technologii komunikacyjnych. Nieupoważniona ingerencja w tę informatyczną infrastrukturę cyberprzestępcy może doprowadzić do ogromnych strat zarówno wynikających bezpośrednio (np. niemożność bieżącego funkcjonowania przedsiębiorstwa) i pośrednio (np. niezrealizowane kontrakty w terminie, utrata dobrego wizerunku firmy) z braku zasilania określonych odbiorców [3].

Złożoność sieci oznacza, że istnieją luki, które jeszcze nie zostały zidentyfikowane. Dlatego trudno jest oszacować ryzyko związane z potencjalnym atakiem ze względu na wielkość, złożoność i dynamiczny charakter sieci energetycznej oraz nieprzewidywalność potencjalnych napastników [3].

Cyber atak ma wyjątkową cechę: może być uruchomiony za pośrednictwem publicznej sieci z odległych miejsc na całym świecie. Dodatkowo może być w formie skoordynowanego ataku z wielu miejsc jednocześnie. Ponadto może atakować różne miejsca jednocześnie [3].

Wykorzystywanie wszelkich rozwiązań do większego wykorzystania inteligentnych sieci, oraz zwiększenie i powielenie ich dróg komunikacji dwustronnej narazi konsumentów i dostawców na więcej form ataków cyberprzestępców. Największe zagrożenia będą występowały po roku 2015 r., kiedy to szacuje się, że inteligentne sieci w Europie obejmą do 440 milionów potencjalnych punktów do ataku hakerskiego.

Cykl życia sieci smart metering to ok. 10–20 lat. Jeżeli w tym czasie zostaną złamane niektóre zabezpieczenia sieci, zwłaszcza urządzeń oraz koncentratorów, to nie będzie możliwości ich wymiany. Nie ma bowiem technicznej możliwości, aby łatwo i tanio wymienić oprogramowanie tych urządzeń w zakresie zwiększenia zabezpieczeń podczas autoryzowania dostępu do danych oraz sterowania urządzeniami. Inteligentne sieci wdrażane dziś mogą doprowadzić za kilka lub kilkanaście lat do katastrofy. Osoba mogąca dwukierunkowo transmitować dane w systemach pomiarowo-rozliczeniowych (smart metering) może w pewnym stopniu sterować licznikami, zabezpieczeniami zalicznikowymi w zakresie odłączania zasilania oraz załączania dodatkowych odbiorów. Dodatkowo może zmienić taryfę przypisaną do licznika i dokonać innych zmian uciążliwych dla odbiorcy oraz wiążących się z koniecznością poniesienia przez niego dodatkowych kosztów.

Przyczyny zagrożeń leżą:

— w lukach systemów operacyjnych, które są potencjalnymi miejscami ataków hackerów,
— po stronie niezadowolonych pracowników, przykładowo zwolniony pracownik może włamać się z chęci zemsty lub sabotażu np. nieprawidłowo zainstaluje oprogramowanie antywirusowe, oraz dostarczy złośliwe oprogramowanie, które będzie siać spustoszenie w inteligentnej sieci. Taki cyberprzestępca zna zabezpieczenia oraz wie, jak je obejść lub jak prawidłowo zautoryzować swój dostęp.

Działanie może polegać na przesyłaniu złośliwego oprogramowania. Dlatego konieczne są odpowiednie certyfikaty oraz zaawansowane metody autoryzacji, które jeżeli nawet nie uniemożliwią, to przynajmniej w znacznym stopniu utrudnią i ograniczą nieautoryzowany dostęp do inteligentnej sieci osobom nieupoważnionym.

Dodatkowo potrzebne jest zaangażowanie dodatkowych firm zajmujących się zarówno zabezpieczaniem sieci, jak również eliminowaniem oraz wykrywaniem działalności cyberprzestępców.

Nie ma takich zabezpieczeń, których nie można byłoby złamać. Niestety nie jest to optymistyczne stwierdzenie. Dlatego warto już teraz, na etapie projektowania systemów inteligentnych sieci, zwrócić uwagę na odpowiedni poziom bezpieczeństwa, możliwości prostej rozbudowy w tym zakresie oraz uwzględnić i przewidzieć potencjalne ataki cyberprzestępców.

6. OCHRONA PRYWATNOŚCI ODBIORCÓW

Inteligentna sieć jest unowocześnieniem istniejących sieci energetycznych. Umożliwia lepszą diagnostykę pracy sieci oraz pozwala sieciom podejmować działania samonaprawcze (oczywiście w określonym zakresie). Dodatkowo umożliwia dynamiczne zintegrowanie lokalnych źródeł energii, w tym również odnawialnej, oraz bardziej efektywnie wykorzystywać energię elektryczną. Zwiększenie automatyzacji i komunikacji w ramach sieci elektrycznej oprócz wielu niewątpliwych zalet ma również, przynajmniej teoretycznie, ciemną stronę: zwiększenie podatności na ataki.

Inteligentne Systemy Licznikowe oraz aplikacje Inteligentnych Sieci muszą być zabezpieczone przed próbami kradzieży tożsamości odbiorcy, danych pomiarowych oraz przed nieautoryzowanym dostępem. Dodatkowo pracownicy OSD lub pracownicy dostawcy oprogramowania mogą chcieć użyć danych personalnych odbiorców do celów innych niż realizacja i rozliczanie dostaw energii, zarządzanie popytem, czy nadzorowanie dokonywanych płatności. Zatem należałoby jakoś ograniczyć możliwość wykorzystania danych osobowych, gromadzonych w bazach w systemach informatycznych w sektorze elektroenergetyki, do celów niezwiązanych z realizacją misji konkretnego przedsiębiorstwa [1].

Niektórych odbiorców niepokoi brak kontroli nad gromadzeniem, przetwarzaniem, dostępem oraz wykorzystywaniem wrażliwych danych osobowych. Problem oczywiście jest nieco szerszy i dotyczy również nieautoryzowanego gromadzenia, pozyskiwania, wykorzystywania i ujawniania innych informacji. Dlatego też potrzebna jest kompleksowa strategia na rzecz ochrony prywatności w Internecie, najlepiej jako część narodowej strategii dostępu do szerokopasmowego internetu [1].

Smart Metering oraz Smart Grid, które jednoznacznie identyfikują poszczególne urządzenia i ich zastosowanie, stwarzają nowe zagrożenia dla prywatności i mogą ujawniać intymne szczegóły życia rodzinnego.

Lista potencjalnych niebezpieczeństw powstałych w wyniku stosowania inteligentnych sieci [1]:

1. Kradzież tożsamości.
2. Ujawnienie osobistych wzorców zachowań (skowronek – rano wstaje, sowa – późno idzie spać, regularny tryb życia, chaotyczny pobór itp.).
3. Gromadzenie i grupowanie odbiorców wg wzorców zachowań.
4. Dostarczanie niechcianych, czasem zawstydzających reklam dobranych na podstawie wzorców zachowań (to tak, jakby dostawca usług internetowych dostarczał reklamy na podstawie listy odwiedzanych stron www; dla niektórych ludzi mogłoby to być krępujące) przykładowo dla osób, u których rejestruje się znaczący pobór energii nocą mogą być przesłane reklamy środków nasennych albo wyższa stawka samochodowego obowiązkowego ubezpieczenia OC – dla towarzystwa ubezpieczeniowego pozbawiony regularnego snu, niewyspany kierowca oznacza większe ryzyko spowodowania przez niego szkody.
5. Możliwość ujawnienia sterowanych urządzeń znajdujących się w danym domu lub mieszkaniu.
6. Decyzje sterowania odbiorami podejmowane na podstawie nieprawidłowych danych, w tym również w skutek działania cyberprzestępców np. hacker sterował pralką lub zmywarką.
7. Nadzór w czasie rzeczywistym, OSD sam może zdecydować o odłączeniu odbiorcy w dowolnym momencie, pod tym względem nie jest nadzorowany przez żadne inne instytucje ani podmioty.
8. Cenzura aktywności – jeżeli OSD mógłby rozpoznawać aktualną aktywność w domu na podstawie pracy określonych urządzeń (określonego zużycia energii bieżącego i historycznego) oraz mógłby zdalnie odłączać zasilanie, to istniałaby pokusa do cenzurowania wykonywania pewnych działalności – ich wykonywanie przez odbiorcę byłoby „nagradzane" przez OSD wyłączeniami zasilania.
9. Monitorowanie zużycia w czasie rzeczywistym – niebezpieczeństwo ujawnienia nieobecności odbiorcy w lokalu mieszkalnym.
10. Ukierunkowanie włamań – dane mogą pokazywać, że pobór energii jest charakterystyczny dla zużycia energii osób w podeszłym wieku, niedołężnych, albo dzieci w wieku wczesnoszkolnym.
11. Zablokowanie odbiorcy dostępu do usług internetowych.
12. Przejmowanie kontroli nad wrażliwymi systemami w zdalnych, słabo kontrolowanych lokalizacjach; czasem może wiązać się to z irytacją ludzi, którzy nie mogą oglądać telewizji lub rozmraża się im lodówka, jednak jeżeli jest mróz takie manipulacje mogą spowodować nawet śmierć niektórych osób.

13. Przechwytywanie danych przez cyberprzestępców oraz manipulowanie inteligentną siecią – zwłaszcza w kwestii sterowania popytem, wyłączania zasilania (w tym również dla prostych domowych systemów alarmowych) lub złośliwego odłączania odbiorcy.
14. Zmanipulowanie cen energii przesyłanych do licznika; przesyłanie np. znacznie zaniżonej ceny energii w godzinach szczytowych oraz wyświetlanie jej u wielu odbiorców może spowodować nawet znaczną zmianę zachowania w kwestii zużycia energii, znaczące zwiększenie zużycia energii przez wielu odbiorców, oszukanych w ten sposób, może być niebezpieczne dla sieci.
15. OSD lub inne instytucje widząc, że pobór energii danego odbiorcy jest większy niż innych, zwłaszcza w godzinach szczytowych może zachęcać ich do oszczędzania energii, naruszając prywatność tego odbiorcy.

Oczywiście należy być świadomym, że nie są to wszystkie możliwe scenariusze, które mogą wystąpić w niedostatecznie zabezpieczonej sieci elektroenergetycznej, w szczególności w nowych sieci inteligentnych.

Należy zdać sobie sprawę, że dane pomiarowe z licznika będą pokazywały określone zachowanie i takie dane będą mogły być wykorzystywane gdzie indziej. Przykładowo takie dane mogłyby być przydatne dla sprzedawcy ubezpieczeń: komunikacyjnych oraz tzw. „na życie". Mógłby on dostosować stawkę ubezpieczenia w zależności np. stopnia uporządkowania profilu odbiorcy, który obrazowałby uporządkowany tryb życia lub bardziej chaotyczny.

Niektórzy odbiorcy wykazują niechęć do udostępniania danych pomiarowych informujących o ich zużyciu energii. Takie dane mogą pokazywać poziom zamożności lub specyficzny pobór energii przez tych klientów. Wyciek takich danych na zewnątrz do podmiotów nieupoważnionych jest zjawiskiem wysoce niepożądanym, ponieważ narusza ich prywatność.

7. PODSUMOWANIE

Zagadnienie bezpieczeństwa inteligentnej sieci pojawia się niejako obok dyskusji o zaletach i korzyściach zaawansowanych technologicznie rozwiązań informatycznych w sektorze elektroenergetycznym. Nie jest to temat nowy. Problematyka z nim związana będzie dynamicznie ewoluowała w zależności od wdrożonych rozwiązań, przyjętych standardów oraz doświadczeń związanych z działalnością cyberprzestępców oraz eliminowania jej skutków.

LITERATURA

[1] Concerning Privacy and Smart Grid Technology, The Smart Grid and Privacy – epic.org/privacy/smartgrid/smartgrid.html

[2] Wilczyński A., Tymorek A. – Rola i cechy systemów informacyjnych w elektroenergetyce, Rynek energii, 2(87)/2010.

[3] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issue, April 2009 – http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf

THE PROBLEMS OF THE CYBER SECURITY OF SMART GRID SYSTEMS

Today, it accentuates the advantages and disadvantages of Smart Grid. Increasingly, it is noted the problem of cyber security. The main threat is the possibility of interference by cyber criminals.Increasing automation and communications within the electricity grid potentially has a dark side; increased vulnerability to attack.