ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

ANNA PAMUŁA
Uniwersytet Łódzki[1]

CYBERPRZESTĘPSTWA W SIECI ELEKTROENERGETYCZNEJ

Streszczenie

Jednym z podstawowych zagadnień związanych z zastosowaniem nowych rozwiązań rynku energii i rozwojem Inteligentnej Sieci Elektroenergetycznej (ISE) jest, oprócz utrzymania stabilności systemu, zapewnienie odpowiedniego bezpieczeństwa jej pracy oraz ochrony danych, zwłaszcza dotyczących odbiorców. W artykule zaprezentowano zagrożenia i potencjalne skutki oraz szkody, na jakie mogą zostać narażeni dostawcy i odbiorcy energii.
Słowa kluczowe: rynek energii, Smart Grid, cyberbezpieczeństwo.

Wprowadzenie

Cyberbezpieczeństwo staje się we współczesnym świecie doktryną, która stanowi podstawę wyznaczającą strategiczne kierunki działań na rzecz bezpieczeństwa w przestrzeni teleinformatycznej, mających zapewnić bezpieczne funkcjonowanie państwa, społeczeństwa, podmiotów gospodarczych oraz obywateli. Zmiana paradygmatu pracy sieci elektroenergetycznej z centralnego na rozproszony, z szeregiem źródeł zasilających oraz znaczącym udziałem aktywnych na rynku energii odbiorców i szeregiem rozwiązań ICT wykorzystujących narzędzia sztucznej inteligencji (Ramchurn i in. 2012), powoduje, iż kwestie bezpieczeństwa stają się jednym z podstawowych elementów decydujących o wdrożeniu nowych rozwiązań. Celem artykułu jest przedstawienie zagrożeń, zwłaszcza cyberataków, jakie stają przed odbiorcami i dostawcami energii. Rozwój tzw. Inteligentnej Sieci Elektroenergetycznej oznacza wprowadzenie do systemu nowej infrastruktury w postaci

[1] Katedra Informatyki.

ogromnej liczy urządzeń i aplikacji pozwalających na dwukierunkową komunikację i interakcję odbiorców z innymi podmiotami rynku energii. Jednocześnie powoduje to wzrost ryzyka potencjalnych ataków na elementy sieci, których skutki mogą kaskadowo rozprzestrzenić się na połączone podsystemy (Khurana i in. 2010). Konsekwencją takich działań mogą być masowe przerwy w dostawach energii, destrukcja urządzeń sieci i sprzętu odbiorców, czy też chaos na rynku energii spowodowany propagacją błędnych sygnałów (na przykład o cenie energii). Liczba cyberataków, których celem jest sektor energetyczny, gwałtownie rośnie (Baker i in. 2010), rośnie również liczba ataków skierowanych na coraz powszechniejsze w użyciu urządzenia mobilne (Symantec 2013). Poziom bezpieczeństwa w sektorze nowej energetyki musi wykraczać poza klasyczne, stosowane do tej pory w biurach i centrach danych rozwiązania i obejmować technologie kontroli sieci, w tym takie technologie, jak: zabezpieczenie systemów typu SCADA i innych systemów czasu rzeczywistego, enkrypcję, ochronę danych i transmisję danych przy pomocy technologii niezbędnych w zaawansowanej infrastrukturze pomiarowej (*Advanced Metering Infrastructure* – AMI) oraz rozwiązaniach informatycznych opartych na modelu chmury obliczeniowej (Pamuła 2013). Budowa Inteligentnej Sieci Elektroenergetycznej wymaga stworzenia dodatkowej infrastruktury komunikacyjno-informatycznej wspomagającej bezpieczeństwo operacji na rynku energii, programów zarządzania popytem na energię czy systemów automatycznego opomiarowania. Bezpieczeństwo pracy sieci, niezawodność dostaw oraz możliwość zarządzania jej pracą są podstawowymi czynnikami prowadzenia tego typu działalności. Jednostki działające w sektorze elektroenergetycznym, w tym dystrybutorzy i dostawcy energii, to przedsiębiorstwa prowadzące określoną politykę bezpieczeństwa, ale rozwój sieci elektroenergetycznych oraz skala i różnorodność związanych z tym wyzwań dotyczących zapewnienia bezpieczeństwa są ogromne (McBridge, McGee 2012). Główne zagrożenia wynikają ze zmiany paradygmatu pracy sieci i są konsekwencją samych jej założeń:

- transmisji poprzez sieć znacznej liczby danych wrażliwych,
- znacznie większej, w stosunku do stanu obecnego, liczby urządzeń do kontroli pracy sieci oraz poszerzenia lub też zmiany standardów wykorzystywanych dotychczas w komunikacji dla celów kontroli zasilania,
- słabego systemu zabezpieczeń znacznej części zainstalowanych urządzeń,
- zmiany standardów komunikacyjnych dotychczas stosowanych i przyłączania do sieci sprzętu głównie poprzez wykorzystanie standardu IP,
- zmiany rynku energii pozwalającej odbiorcom na masowy w nim udział.

Stopień zależności sieci elektroenergetycznej od rozwiązań ICT nieustanie rośnie. Zaburzenia w systemie komunikacyjnym przekładają się na zaburzenia w systemie elektroenergetycznym; podobna sytuacja ma miejsce w przypadku odwrotnym (Pearson 2011). Na ataki narażone są wszystkie elementy infrastruktury,

a szczególnie istotne staje się bezpieczeństwo danych gromadzonych i przesyłanych przez systemy inteligentnego opomiarowania (Efthymiou i in. 2010).

Intensywne działania w tym zakresie podejmowane są przez Unię Europejską (Pearson 2011). W USA w wytycznych wydanych przez NIST[2], dotyczących bezpieczeństwa dla nowej sieci elektroenergetycznej, wyróżniono 3 główne obszary wzmocnienia działań:

- dostępność – zapewnienie terminowego i niezawodnego dostępu do danych i korzystanie z informacji istotnych dla zarządzania siecią i rynkiem energii,
- integralność – ochrona przed niepowołaną modyfikacją lub zniszczeniem oraz zapewnienie wiarygodności i autentyczności,
- poufność – zapewnienie autoryzowanego dostępu do informacji, zwłaszcza dotyczących osób prywatnych.

Bezpieczeństwo infrastruktury dotyczy zarówno sfery transmisji i dystrybucji energii, będącej w gestii dostawców, jak również obszaru inteligentnego opomiarowania, który może być obsługiwany przez inne podmioty rynku czy infrastruktury domowej gospodarstw domowych oraz urządzeń wykorzystywanych przez odbiorców, obejmując więc wiele aspektów, takich jak (McBridge, McGee 2012):

- zabezpieczenie fizyczne samych przedsiębiorstw, zainstalowanego sprzętu i sieci elektroenergetycznej,
- bezpieczeństwo pracy sieci komputerowej,
- bezpieczeństwo pracy organizacji,
- bezpieczeństwo pracy systemów SCADA,
- bezpieczeństwo pracy punktów końcowych sieci elektroenergetycznej.

Internet jest swego rodzaju paradygmatem dla projektowania infrastruktur o dużej skali, niemniej jednak tworzenie sieci komunikacji dla potrzeb zarządzania w elektroenergetyce wymaga stworzenia bardzo pewnego, wydajnego i bezpiecznego systemu sterowania urządzeniami zainstalowanymi w infrastrukturze. Istnieją określone różnice w komunikacji za pomocą sieci Internet a komunikacją w ISE, dotyczące między innymi obszarów (Wang i in. 2013):

- czasu transmisji danych (ISE: czas krytyczny 3 ms lub mniej, Internet: 100 ms lub mniej),
- natężenia ruchu (ISE: okresowe, Internet: narastające, potęgowe),
- metryk wydajności (ISE: przepustowość, rzetelność, Internet: opóźnienie komunikatu),
- modelu komunikacji (ISE: dwukierunkowa, peer-to-peer, Internet: end-to-end),
- protokołów (ISE: własne, heterogeniczne, Internet: IPv4 i IPv6).

Funkcjonalność urządzeń i aplikacji ISE nie może być wdrażana bez zapewnienia odpowiedniego poziomu bezpieczeństwa. Wszystkie strony biorące udział w rynku energii (dystrybutorzy, agregatorzy, dostawcy usług dodatkowych) muszą

[2] National Institute of Standards and Technology, http://www.nist.gov.

zapewniać poufność przechowywania i przesyłania danych. Idea ISE oznacza nowe funkcjonalności i nowe rozwiązania biznesowe, ale jednocześnie stwarza nowe zagrożenia z punktu widzenia bezpieczeństwa, co może prowadzić do konfliktu: nowa funkcjonalność *versus* bezpieczeństwo. Nowe rozwiązania muszą zapewniać równowagę, tzn. system powinien funkcjonować w sposób poprawny, nie pozwalając na nadużycia i bezprawne wykorzystanie.

1. Cele funkcjonowania sieci elektroenergetycznej a zapewnienie bezpieczeństwa

Nadrzędnym celem pracy sieci jest dostarczanie energii odbiorcom w sposób niezawodny. System bezpieczeństwa musi być odpowiedzialny za zapobieganie atakom prowadzonym zarówno przez czynnik ludzki, jak i środowiskowy, minimalizując negatywne skutki tych ataków, a tym samym poprawiając niezawodność działania. Analiza danych w ISE pełni kluczową rolę, a zatem zapewnienie integralności, poprawności i dokładności przesyłanych danych ma znaczenie podstawowe. Nowy model pracy sieci zakłada rozproszenie źródeł zasilania, co oznacza masową liczbę instalacji odnawialnych źródeł energii. Instalując takie źródło klient może podjąć decyzję o sprzedaży energii. Odbiorca tej energii musi mieć pewność, że płaci za rzeczywiście przesłaną energię (dane muszą być rzetelne), stąd niezbędne są odpowiednie mechanizmy kontroli dla integracji danych i urządzeń w sieci.

Kolejnym celem wdrażania rozwiązań ISE jest redukcja emisji gazów cieplarnianych. Jednym ze sposobów redukcji jest ograniczenie zużycia energii. Odbiorcy będą otrzymywać na bieżąco dane na temat konsumpcji energii, co może zachęcić ich do zmiany przyzwyczajeń w korzystaniu z niej. Zgodnie z zasadami ochrony prywatności wszystkie dane na temat klienta, jego urządzeń, profilu muszą być zabezpieczone przez zastosowanie odpowiednich narzędzi kontroli i szyfrowania.

Innym istotnym typem zagrożenia dla odbiorcy są przerwy w zasilaniu. Zagrożenia związane z przerwami zasilania w systemie elektroenergetycznym można podzielić na kilka kategorii (Flick, Morehouse 2011; Pamuła 2013):

1. Zagrożenia związane z pogodą i innymi czynnikami naturalnymi – silne wiatry, opady, oblodzenie to czynniki, które mogą prowadzić do uszkodzeń linii doprowadzających energię do budynków mieszkańców.
2. Zagrożenia związane z atakami na zaawansowaną infrastrukturę i urządzenia zainstalowane w sieci domowej, które mogą wykorzystać jako furtki do ataku na inne urządzenia całej sieci, najczęściej dokonywane poprzez:
   - śledzenie zachowania i stylu życia osoby poprzez szczegółową analizę danych o zwyczajach konsumenta, np. na portalach, gdzie klienci mogą monitorować swoje zużycie energii lub porównywać je z innymi (udostępnianymi przez dostawców lub na innych portalach);

- ataki hakerskie, których motywacja jest podobna do ataków na inne systemy (motywy ambicjonalne, testowanie systemu).

Dla prawidłowej pracy sieci elektroenergetycznej szczególne zagrożenie stanowi kategoria wirusów, które zatrzymują pracę systemu lub baz danych, w celu wymuszenia okupu na właścicielach lub użytkownikach (tzw. ataki DoS) (Wang 2013). Przystosowanie tego typu wirusów do przejęcia kontroli nad urządzeniami, takimi jak inteligentny licznik, może zablokować dostęp użytkownika do zasilania energią. Powodem takich działań mogą być motywy psychologiczne (osobowościowe), takie jak: chęć zemsty, kłótnie sąsiedzkie, zazdrość itp. A działania te mogą prowadzić do wyłączenia lub przejmowania kontroli nad licznikami. Osobnym zagrożeniem jest terroryzm – atakując sieć elektroenergetyczną terroryści mogą mieć wpływ na bardzo wielu użytkowników. Zagrożenie to dotyczy zarówno fizycznego uszkodzenia sieci, jak i systemów zarządzania.

Każde z potencjalnych zagrożeń, oprócz braku zasilania, może mieć dla dostawcy i klienta-użytkownika energii negatywny skutek finansowy. Przekłamanie danych z infrastruktury inteligentnego opomiarowania spowoduje wzrost wysokości rachunków klientów, nawet jeśli może to być wzrost dla odbiorcy niezauważalny.

2. Dostawcy energii a zapewnienie bezpieczeństwa pracy systemu

Większość działań zapewniających bezpieczeństwo leży po stronie dostawców energii oraz w odpowiednich rozwiązaniach prawnych. Z punktu widzenia dostawcy kluczowym elementem zarządzania bezpieczeństwem jest zmniejszenie kosztów związanych z jego zapewnieniem, które oprócz kosztów podstawowych obejmują koszty związane z jego naruszeniem (McBridge, McGee 2012) w tym: koszty osobowe, koszty naprawy lub zakupu urządzenia, koszty oprogramowania czy koszty administracyjne. Zarządzanie bezpieczeństwem wymaga prowadzenia działań analitycznych kalkulujących koszty zabezpieczeń wraz z kosztami naruszenia bezpieczeństwa, w oparciu o ocenę ryzyka wystąpienia i potencjalnych skutków.

Kompleksowość i koszty zapewnienia bezpieczeństwa będą rosły wraz z rozwojem sieci elektroenergetycznej, zwłaszcza że wprowadzane rozwiązania są nowe i mogą mieć wiele „luk", pozwalających na naruszenie bezpieczeństwa. Przedsiębiorstwa energetyczne, aby zapewnić bezpieczeństwo pracy systemu, będą musiały prowadzić działania w wielu kierunkach związanych z monitorowaniem zagrożeń prowadzących do utraty ich wiarygodności biznesowej (McBridge, McGee 2012):

- utrata kontroli nad bieżącą pracą sieci – bezpieczna, niezawodna i prowadzona w czasie rzeczywistym kontrola pracy sieci jest podstawą działania dostawców energii; zagrożenie stanowią przypadkowe i celowe uszkodzenia urządzeń;

- kradzieże energii (tzw. straty nietechniczne) związane z nielegalnym poborem lub włamaniem i zmianą danych w licznikach lub systemach informatycznych prowadzące do błędnego naliczania rachunków;
- zmiany danych i odmowa świadczenia usług w wyniku działania wirusów; zagrożenie to jest tym większe im większa jest liczba dołączanych do sieci urządzeń, np. komputerów i urządzeń mobilnych wykorzystywanych do zarządzania wykorzystaniem energii przez odbiorców;
- naruszenia zasad bezpieczeństwa danych osobowych odbiorców podczas przesyłu lub w miejscu ich gromadzenia – wystąpienie tego zagrożenia może powodować nie tylko utratę wizerunku firmy, ale też sankcje karne;
- infiltracja sieci przez strony i osoby nieuprawnione;
- nieuprawniony, nieautoryzowany dostęp do sieci, danych czy aplikacji.

W tabeli 1 zamieszczono główne zagrożenia i potencjalne skutki ataków dla odbiorcy i dostawcy energii.

Tabela 1

Zagrożenia, cele i rezultaty ataków odbiorców i dostawców energii

Zagrożenie	Cel i typ ataku	Skutek
Kradzież danych osobowych. Włamanie do bazy poprzez strony internetowe.	Modyfikacja bazy danych.	Przejęcie danych osobowych klientów, numerów kont, kart. Sprzedaż danych.
Przejęcie i fałszowanie danych o konsumpcji energii. Pozbawienie konsumentów praw.	Zmiana danych profilu odbiorcy w celu ukrycia bądź ukazania obecności w określonym miejscu i czasie.	Obowiązek dostarczenia na życzenie odpowiednich organów państwowych żądanych danych.
Naruszenie praw własności do informacji danych osobowych klientów, umów handlowych, strategii itd.	Zasoby organizacji poprzez programy, np. przeglądarki internetowe z brakiem aktualizacji.	Przejęcie danych z systemu. Instalacja wrogiego oprogramowania. Ujawnienie danych handlowych i planów.
Publikacja w Internecie metod dostępu do urządzeń pomiarowych. Masowe oszustwa zawiązane z przesyłaniem nieprawidłowych danych o zużyciu energii.	Urządzenia infrastruktury pomiarowej. Instalacja nielegalnych programów pozwalających na przesłanie zaniżonych danych o zużyciu energii.	Masowe zaniżanie rachunków. Masowe zawyżanie ilości energii oddawanej do sieci. Straty finansowe dostawcy. Obciążanie kosztami innych klientów.
Publikacja metod dostępu do urządzeń i sensorów sterowania siecią, np. związanych z przekierowaniem energii, wyłączeniem fragmentu sieci czy odtworzeniem po zaniku zasilania.	Urządzenia sieciowe. Dane przesyłane z sensorów urządzeń pomiarowych do dostawcy w postaci niezaszyfrowanej.	Przesyłanie fikcyjnych danych np. o braku zasilania. Koszty związane z obsługą nieistniejących awarii. Obciążanie kosztami innych klientów.
Przejęcie haseł do urządzeń domowych przez znajomych.	Przejęcie haseł do sieci domowej, chęć uprzykrzenia życia, zabawa.	Zmiana haseł. Odcięcie zasilania. Utrudnienie w zarządzaniu zużyciem energii.
Nieuprawniony dostęp do danych przez zwolnionego pracownika.	Wykorzystanie haseł i znanych metod dostępu do systemu w celu manipulacji.	Zamknięcie konta. Manipulacja danymi.
Przejęcie haseł do kont przez hakerów i osoby obce.	Instalacja oprogramowania skanującego hasła i konta, e-maile z wirusami.	Manipulacja danymi konta. Zmiana profilu zużycia energii.

Źródło: opracowanie na podstawie (Flick, Morehouse 2011; Pamuła 2013).

Mnogość potencjalnych zagrożeń spowodowała, iż podejmowane są próby tworzenia taksonomii ataków dla rozwijającej się sieci elektroenergetycznej łączą-

cej wiele heterogenicznych systemów, w dużej części korzystających z technologii agentowych do kontroli działania (Hu i in. 2014).

3. Gromadzenie i przesyłanie danych osobowych

System komunikacji w Inteligentnej Sieci Elektroenergetycznej wymaga gromadzenia, przetwarzania i przesyłania danych osobowych, w tym tzw. danych wrażliwych. Z punktu widzenia bezpieczeństwa ważne jest określenie, które dane, w jakich odstępach czasu oraz w jaki sposób będą przesyłane do dostawcy i firm TPA[3], a także które z nich będą uznawane jako obowiązkowe, a które dobrowolne i przetwarzane za zgodą użytkownika. Odbiorca musi mieć pełną informację o tym, kto i w jakim celu korzysta z danych o nim.

Wielu konsumentów energii nie zdaje sobie sprawy z tego, jakie dane są zbierane i gromadzone w systemie inteligentnego opomiarowania oraz udostępniane innym firmom. Wykorzystanie danych osobowych w celach innych, niż były one zbierane, wymaga specjalnej uwagi z punktu widzenia ochrony danych osobowych, jako że może zaistnieć ryzyko przejmowania pakietów danych o odbiorcy i jego urządzeniach (Cavoukian i in. 2010). Podobnie rzecz się ma z wykorzystywaniem sieci i portali społecznościowych do udostępniania klientom możliwości monitorowania danych o zużyciu energii. Jest to wygodne rozwiązanie z punktu widzenia marketingowego, ale niestety ryzykowne z punktu widzenia bezpieczeństwa tych danych, jako że pomimo stosowania zabezpieczeń zanotowano przypadki ich skutecznego łamania (Pamuła 2013).

Ataki, których celem będą odbiorcy energii, mogą ulec nasileniu w momencie większego udziału na rynku usług firm trzecich, kiedy odbiorcy będą mogli zdalnie zarządzać urządzeniami poprzez swoją sieć domową. Istotne jest więc stworzenie równowagi pomiędzy korzyściami wynikającymi z rozszerzonych możliwości komunikacyjnych z jednej strony, a zachowaniem prywatności odbiorców z drugiej. Usługi z zakresu ochrony i bezpieczeństwa sieci domowej mogą stać się dodatkową ofertą dostawców energii dla klientów, stanowiącą dla nich źródło istotnych przychodów (Pamuła 2013). Znaczenie, jakie dla odbiorcy ma ochrona i bezpieczeństwo, oraz wysokość budżetu, jaki jest w stanie przeznaczyć na ten cel, może być jedną z podstaw prowadzenia segmentacji ofert sprzedaży energii powiązanych z ofertą dodatkową. Badanie preferencji odbiorców w tym obszarze wiąże się z tworzeniem systemu miar „prywatności" (Ratliff i in. 2014).

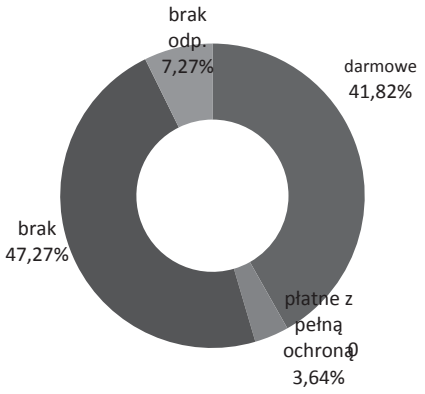
W celu zabezpieczenia danych w systemach inteligentnego opomiarowania proponowane jest już szereg rozwiązań, takich jak: stosowanie odpowiednich standardów (Wang i in. 2013, Metke i in. 2010), anonimizacja danych (Efthymiou

[3] Na rynku energii obowiązuje zasada Third Party Access (TPA).

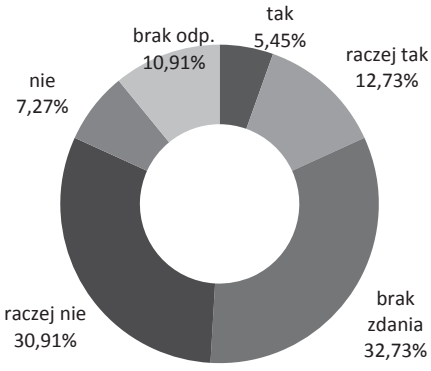
2010), wykorzystanie algorytmu nieinwazyjnego monitorowania NILM[4] (Ratliff i in. 2014). Budowa systemu bezpieczeństwa danych wymaga podejścia holistycznego, wykorzystującego odpowiednio przygotowane narzędzia oparte na koncepcji infrastruktury klucza publicznego (Metke i in. 2010).

4. Odpowiedzialność odbiorcy energii za bezpieczeństwo systemu

Urządzenia mobilne są coraz częściej i powszechniej używane w celu dostępu do informacji, zarządzania płatnościami, w celach biznesowych czy też rozrywkowych i towarzyskich. Podobnie aplikacje tworzone do zarządzania wykorzystaniem energii dostępne będą nie tylko na licznikach i panelach domowych, ale właśnie na urządzeniach mobilnych. Odpowiedzialność odbiorców za bezpieczeństwo systemu odnosi się między innymi do prawidłowego zabezpieczenia tych urządzeń i postępowania zgodnie z zasadami przyjętymi przez dostawcę, np. ustalania silnych haseł dostępowych czy nieudostępniania danych do kont, stosowania oprogramowania antywirusowego.



Rys. 1. Wykorzystanie programów antywirusowych na urządzeniach mobilnych



Rys. 2. Czy aplikacje do zarządzania energią w domu będą bardziej narażone na ataki niż inne (np. bankowe)?

Źródło: opracowanie własne na podstawie badań.

W badaniach przeprowadzonych wśród studentów kierunków Zarzadzanie, Finanse i Logistyka Uniwersytetu Łódzkiego na przełomie 2014 i 2015 roku prawie 42% respondentów uznało, że przesyłanie przez inteligentne liczniki danych zwią-

[4] *Nonintrusive load monitoring* – algorytm pozwalający na podstawie analizy zmian napięcia na określenie, jakie urządzenia pobierające energię są wykorzystywane przez odbiorcę.

zanych z wykorzystaniem energii przez urządzenia domowe nie budzi ich obaw. Jedynie około 5,5% respondentów uznało, iż tego typu aplikacje mogą być bardziej narażone na ataki (rysunek 2). W tej samej grupie prawie 48% badanych przyznało, że nie korzysta z programów antywirusowych na urządzenia mobilne (rysunek 1). 80% respondentów wyraziło opinię, że o bezpieczeństwo i ochronę danych przesyłanych dla potrzeb zarządzania wykorzystaniem energii na urządzenia mobilne powinien dbać dostawca aplikacji, około 50% było zdania, iż odpowiedzialność leży po stronie dostawcy energii. Jednocześnie prawie 53% respondentów uznało współodpowiedzialność właściciela urządzenia.

Odbiorcy energii będą nadal w dużym stopniu uzależnieni od sieci elektrycznej i dostawców energii, we wszystkich aspektach codziennego życia, związanego z korzystaniem z urządzeń zasilanych prądem. Zmiany paradygmatu pracy sieci elektroenergetycznej spowodują, że konsumenci będą narażeni na nowe zagrożenia, np. w postaci ataków hakerskich na własną, domową sieć. Aby zapobiegać zagrożeniom i minimalizować ich skutki, odbiorcy będą liczyć na dostawców i organy prawne. Nie mniej istotne jest, aby wykorzystywali dobre praktyki, np. stosując oprogramowanie antywirusowe czy silne hasła dostępu do systemu.

Podsumowanie

Bezpieczeństwo rozwijającej się sieci elektroenergetycznej stanowi kombinację wielu czynników: działań dostawców, odbiorców, dostawców aplikacji i usług oraz prowadzonej przez państwo polityki ochrony w cyberprzestrzeni.

Nowoczesne technologie informatyczno-komunikacyjne stanowią nie tylko udogodnienie w życiu konsumentów, ale też zagrożenie. Energia jest dobrem podstawowym, bez którego większość konsumentów nie jest w stanie funkcjonować. Praktycznie nie ma możliwości stworzenia w 100% całkowicie bezpiecznej aplikacji czy sieci i rozwijająca się sieć elektroenergetyczna nie będzie w tym zakresie wyjątkiem. Poufność, dostępność, integralność i wiarygodność danych są to czynniki stanowiące podstawę bezpieczeństwa informacji i muszą być zaimplementowane w sposób satysfakcjonujący, tak aby nowe rozwiązania mogły być bezpieczne i funkcjonalne.

Literatura

1. Baker S., Filipiak N., Timlin K. (2010), *In the Dark: Crucial Industries Confront Cyberattacks*, McAfee Second Annual Critical Infrastructure Protection Report Written with the Center for Strategic and International Studies (CSIS), McAfee, http://www.mcafee.com/us/resources/ reports/rp-critical-infrastructure-protection.pdf.

2. Cavoukian A., Polonetsky J., Wolf C. (2010), *Smart privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Identity in the Information Society, August, Volume 3, Issue 2, pp 275-294, IDIS, 3, Springer, DOI: 10.1007/s12394-010-0046y.
3. Efthymiou C., Kalogridis G. (2010), *Smart Grid Privacy via Anonymization of Smart Metering Data*, First IEEE International Conference on Smart Grid Communications, Gaithersburg 4-6 Oct., IEEE, 978-1-4244-6511-8/10.
4. Flick T., More House J. (2011), *Securing the Smart Grid. Next Generation Power Grid Security*, Syngress.
5. Hu J., Pota H.R, Guo S. (2014), *Taxonomy of Attacks for Agent-Based Smart Grid*, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 7, July.
6. Khurana H., Hadley M., Lu N., Frincke D.A. (2010), *Smart-Grid Security Issues*, IEEE Security and Privacy, co-published by the IEEE Computer and Reliability Societies, January/February.
7. McBride A., McGee A.R. (2012), *Assessing Smart Grid Security*, Bell Labs Technical Journal 17(3), 87–104 Wiley Periodicals online Wiley Online Library (wileyonlinelibrary.com) DOI: 10.1002/bltj.21560.
8. Metke A.R., Ekl R.L. (2010), *Security Technology for Smart Grid Networks*, IEEE Transactions on Smart Grid, Vol. 1, No. 1, June.
9. Pamuła A. (2013), *Zaangażowanie odbiorców z grupy gospodarstw domowych w zarządzanie popytem na energię*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź.
10. Pearson I.L.G. (2011), *Smart Grid Cyber Security for Europe*, Energy Policy 39.
11. Ramchurn S.D., Vytelingum P., Rogers A., Jennings N.R. (2012), *Putting the 'Smarts' into the Smart Grid: A Grand Challenge for Artificial Intelligence*, Communications of the ACM, April, vol. 55, No. 4, DOI:10.1145/ 2133806.2133825.
12. Ratliff L.J., Dong R., Ohlsson H., Cardenas A.A., Sastry S.S., *Privacy and Customer Segmentation in the Smart Grid.* http://www.eecs.berkeley.edu/~ratliffl/ Research/papers/2014CDC.pdf.
13. Symantec, *Internet Security Threat Report 2013*, Vol. 18, 2013.
14. Wang W., Lu. Z., (2013), *Cyber Security in the Smart Grid: Survey and Challenges*, Computer Networks 57.

CYBER ATTACKS IN SMART GRID

Summary

One of the basic Smart Grid challenge is to supply energy via the complex strongly ICT depended system with more efficiency and reliability ensuring at the same time high level of security. Because of its new dispersed and heterogeneous nature the Smart Grid is exposed to different type of cyber-attacks. The main objective of this paper is to provide a look of basic threatens and their impact to utilities and energy consumers.

Keywords: energy market, Smart Grid, cyber security.

Translated by Anna Pamuła