Kamil Kowalczuk, ekspert ds. bezpieczeństwa automatyki przemysłowej,
Łukasz Ślęzak, ekspert ds. bezpieczeństwa danych osobowych, PricewaterhouseCoopers Sp. z o.o.

Inteligentne sieci a cyberataki

- czy zagrożenie jest realne?

Bezpieczeństwo cybernetyczne staje się jednym z najważniejszych wyzwań dla systemów energetycznych, które są coraz bardziej narażone na cyberataki. Słowa te są samospełniającą się przepowiednią. A teraz przejdźmy do faktów.

W 2016 r. 40 mln ludzi w Turcji było odcięte od prądu - istnieją dowody na przeprowadzenie cyberataku. W grudniu 2015 r. ukraińskie przedsiębiorstwa doświadczyły nieplanowanych przerw w dostawie prądu. BlackEnergy malware został odkryty w sieciach komputerowych przedsiębiorstw z różnych sektorów infrastruktury energetycznej - zagrożenia dotyczyło również polskich przedsiębiorstw.

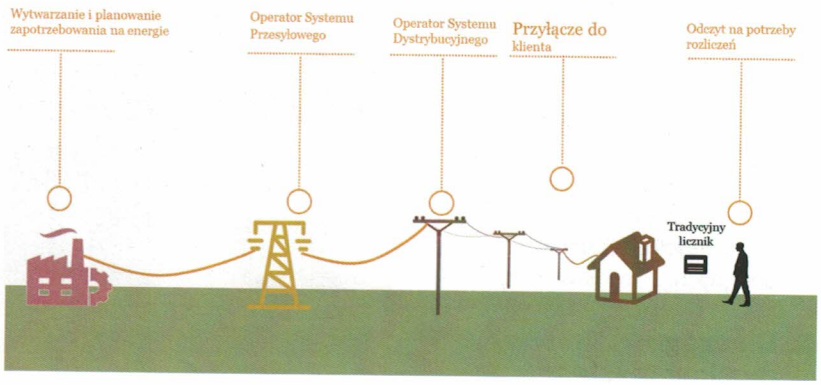
Czym właściwie jest inteligentna sieć (ang. *Smart Grid*) i dlaczego zmienia sposób widzenia?

Przyjmuje się, że inteligentna sieć energetyczna (dotyczy całego sektora elektroenergetycznego) ma na celu dostarczenie odbiorcom energii elektrycznej przy wsparciu infrastruktury IT. Możliwe jest również użycie jej na potrzeby innych mediów (gaz, woda). Sieci tego typu zapewniają obniżenie kosztów i zwiększenie efektywności oraz zintegrowanie rozproszonych źródeł energii (w szczególności mowa tutaj o odnawialnych źródłach energii). Różnice w podejściu zilustrowano na rysunku 1 i 2.

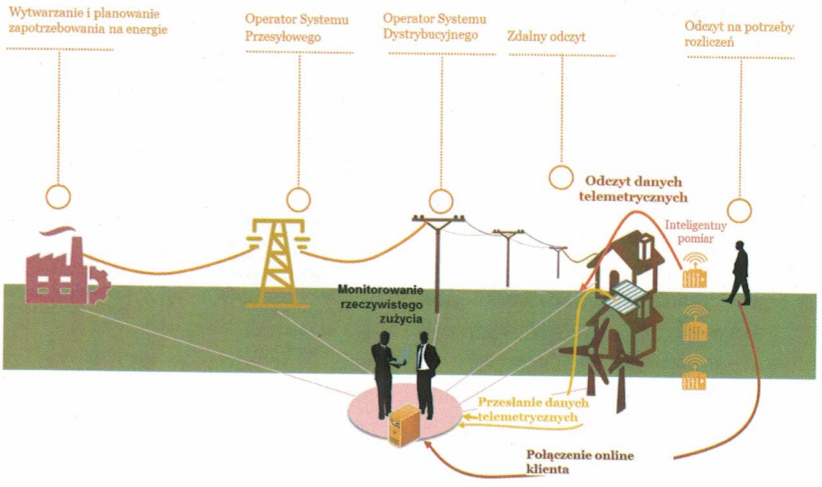
Rozwój elektroenergetyki w kierunku inteligentnych sieci stał się faktem. Możliwości zastosowania i wykorzystanie nowych technologii w elektroenergetyce umożliwiło wniesienie nowej jakości. Sieci tego rodzaju pozwalają na komunikację i interakcję pomiędzy wszystkimi interesariuszami w zakresie przesyłanych danych pomiarowych i rozliczeniowych. Można pokusić się o stwierdzenie, że inteligenta sieć energetyczna przechodzi metamorfozę z wolnozmiennych stanów (zapotrzebowania na tzw. grafikowanie ustala się odpowiednio wcześniej) do dynamicznego reagowania na zapotrzebowanie (reagowanie na potrzeby omal w czasie rzeczywistym). Pozwala to ograniczyć straty na przesyle oraz podnieść efektywność sieci elektroenergetycznej, między innymi poprzez integrację źródeł energii i optymalizację sieci (ograniczamy np. straty na przesyle do punktu docelowego). Zastosowanie takiego podejścia do budowania sieci pozwala na szybkie reagowanie na zmieniające się otoczenie i dostarczenie klientom lepszej jakości usługi.

Główne zalety budowania inteligentnych sieci to:

- usprawnienie rozliczeń,
- mniejsze koszty wynikające z korygowania błędów,



Rys. 1. Tradycyjny model sieci przesyłowej



Rys. 2. Model inteligentnej sieci

Tab. 1. Różnice pomiędzy tradycyjnym modelem sieci, a siecią inteligentną:

TRADYCYJNA SIEĆ	INTELIGENTNA SIEĆ
Systemy automatyki przemysłowej i systemy klienckie są oddzielone	Systemy automatyki przemysłowej i klienckie są ze sobą połączone
Tradycyjne podejście służy jedynie do kontroli	Systemy inteligentne umożliwiają podejmować decyzje o stanach sieci, modelować ją i zwiększać efektywność poprzez optymalizację na podstawie rzeczywistych potrzeb
Tradycyjne sieci pozwalały na wysłanie poleceń i otrzymanie aktualizacji stanu	Poza wysłaniem polecenia mamy aktualizację na bieżąco, a ponadto umożliwia nam to przechowywanie i przetwarzanie informacji - proaktywnie reagować na zmiany zachodzące w sieci
Rozdzielenie tradycyjnego pomiaru i optymalizacja sieci oparta na prognozowaniu	Komunikacja dwukierunkowa w czasie rzeczywistym
AMR (ang. *Automatic Meter Reading* - automatyczny odczyt liczników) - pierwotnie urządzenia, które pobierały dane rozliczeniowe dla odpowiedniego klienta. Pozwalały również na zdalne alarmowanie o próbie manipulowania licznikiem czy inne awaryjne zdarzenia.	AMI (ang. *Advanced Metering Infrastructure* - zaawansowana infrastruktura pomiarowa) - jest to szereg elementów, w tym inteligentne liczniki, koncentratory i rejestratory, elementy pozwalające na dwukierunkową komunikację z Zakładem Energetycznym (AMI jest elementem Smart Grid). Celem AMI jest zapewnienie przedsiębiorstwu rzeczywistych danych o zużyciu energii, w tym informacje geograficzne. Możliwość dokonywania świadomych wyborów w czasie rzeczywistym przez klienta o zużyciu energii, w oparciu o ceny, w trakcie użytkowania.

- dokładny odczyt liczników, bez potrzeby prognozowania - przejrzystość odczytu,
- mniejsze koszty pracy oraz czas uzyskania danych pomiarowych,
- optymalizacja sieci elektroenergetycznej - zwiększenie efektywności, w szczególności dla sieci dystrybucyjnych.

Dlaczego musimy myśleć o bezpieczeństwie w przypadku inteligentnych sieci?

Rozważmy podstawowe przypadki użycia systemu inteligentnego opomiarowania:

- wielu klientów zgłasza zapotrzebowanie z siedziby klienta i otrzymuje automatycznie dostęp do mediów (energia, gaz, woda);
- określenie zdalnie limitu klienta i możliwość zdalnego rozłączenia lub załączenia usługi u klienta;
- urządzenie u klienta wykrywa włamanie do sieci elektroenergetycznych po stronie klienta;
- odczyt zdalny stanu licznika u klienta.

Nieupoważniona ingerencja w infrastrukturę przez cyberprzestępcę może doprowadzić do strat zarówno wynikających bezpośrednio, jak i pośrednio z braku zasilania u odbiorców. Złożoność sieci powoduje ryzyko istnienia luk, które jeszcze nie zostały zidentyfikowane.

Do tej pory, przed wdrożeniem rozwiązań Smart Grid, ochrona w zakresie liczników koncentrowała się głównie na bezpieczeństwie fizycznym, czyli np. właściwym zabezpieczeniem stacji transformatorowych. Teraz dochodzą dodatkowe problemy, które dobrze znane są np. w sektorze bankowym lub u operatorów telekomunikacyjnych. Związane są z zapewnieniem bezpieczeństwa przetwarzanych danych - zabezpieczeniem wszystkich operacji wykonywanych na danych, takich jak: zbieranie, utrwalanie, przechowywanie,

Przepływ danych niezbędnych do prawidłowego funkcjonowania zaawansowanego inteligentnego pomiaru:

Rys. 3. Model przepływu danych

Można wskazać cztery główne obszary, w których może nastąpić zagrożenie cyberatakiem:

Zagrożenia i podatności:

opracowywanie, zmienianie, udostępnianie i usuwanie. Na rys. 3. pokazano, schemat przepływu danych w nowym podejściu.

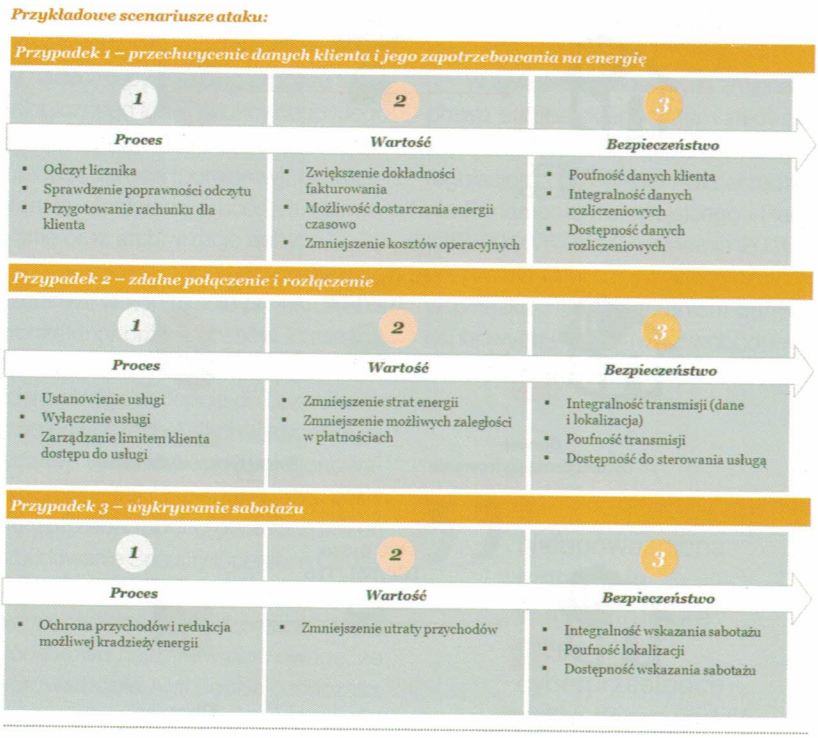
Przykładem niedawnego cybeataku w sektorze energetycznym było podszycie się pod Biuro Obsługi Klienta jednej z największych grup energetycznych w kraju i masowe wysłanie faktur za energię. Osoby, które postąpiły zgodnie z wiadomością w rezultacie miały zaszyfrowane pliki na dyskach swoich komputerów (Crypt0L0cker). Można założyć, że podobny scenariusz lub podszycie się pod portal klienta będzie coraz częściej spotykane w sektorze.

> Rozwój elektroenergetyki w kierunku inteligentnych sieci stał się faktem. Możliwości zastosowania i wykorzystanie nowych technologii w elektroenergetyce umożliwiło wniesienie nowej jakości

Zaszyfrowanie danych bez możliwości odszyfrowania, przechwycenie danych klienta, przejęcie sterowania czy brak informacji o próbie nielegalnego podłączenia się do sieci energetycznej - to tylko niektóre z możliwych scenariuszy ataku, uszczegółowione na rysunku 4.

Światowe standardy opisują bezpieczeństwo jako zapewnienie pewnych atrybutów. Podstawowe atrybuty bezpieczeństwa informacji to:

Przy tradycyjnych systemach automatyki przemysłowej na pierwszym miejscu jest dostępność i integralność danych. W przypadku Smart Grid równie ważna jest poufność uzyskiwanych



Rys. 4. Scenariusze ataku

danych pomiarowych, jak i ich lokalizacja geograficzna (z jakiego źródła pochodzą informacje).

W bezpieczeństwie wyróżniamy trzy podstawowe atrybuty informacji:

Poufność - atrybut bezpieczeństwa wskazująca, że dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom. W odniesieniu do naszej organizacji jest to zapewnienie odpowiedniego poziomu dostępu do informacji, niezbędnego z punktu widzenie wykonywanych obowiązków. Przykładem jest dostęp do danych przechowywanych w Systemie Dyspozytorskim oraz zapewnienie go wyłącznie osobom, które ze względu na charakter swojej pracy muszą je przetwarzać.

Integralność - atrybut bezpieczeństwa wskazujący, że dane nie uległy zniekształceniu (nie zostały zmienione, dodane lub usunięte) w nieautoryzowany sposób. Przykładem jest proces wymiany danych pomiędzy dwoma odrębnymi systemami lub systemem a operatorem (HMI). W procesie ich uzyskiwania nie nastąpiła niekontrolowana zmiana, np. poprzez błąd systemu lub działanie szkodliwego oprogramowania ingerującego w system. Integralność jest niezwykle istotna dla systemów transakcyjnych, sterowania oraz obrazowania. W badanym obszarze integralność danych ma również znaczenie w zakresie przekazania informacji niskopoziomowo np. pomiędzy PLC (urządzenie przeznaczone do sterowania pracą maszyny lub urządzeń) i Systemem Dyspozytorskim.

Dostępność - atrybut bezpieczeństwa wskazujący, że w określonym czasie i miejscu użytkownik może uzyskać wymaganą informację. Podstawowym przykładem jest uzyskanie informacji z systemu automatyki przesyłowej przez użytkownika czy inny system.

Przy tradycyjnych systemach automatyki przemysłowej na pierwszym miejscu jest dostępność systemu i integralność danych. W przypadku Smart Grid równie ważna jest poufność uzyskiwanych danych pomiarowych oraz ich lokalizacja geograficzna (z jakiego źródła pochodzą informacje).

Smart Grid wprowadza potrzebę podejścia holistycznego do bezpieczeństwa i budowania go w sposób zbliżony dla typowych systemów rozproszonych spotykanych szeroko w sektorze finansowym oraz telekomunikacyjnym, oraz budowania świadomości u odbiorców.

Podstawowe wyzwania w Cyberbezpieczeństwie dla Smart Grid zgodnie z opracowaniem U.S. Department of Energy to:

- niepełne zrozumienie potencjalnych zagrożeń,
- trudność w oszacowaniu kosztów zmaterializowania się zagrożenia,
- brak jednolitego standardu oceny bezpieczeństwa,
- ograniczony dostęp do informacji o nowych podatnościach,
- przeświadczenie, że bezpieczeństwo jest drogie,
- zwiększenie wykorzystania otwartych systemów operacyjnych.

Jak podejść do zaprojektowania bezpiecznej inteligentnej sieci?

Powstaje wiele opracowań w kontekście bezpieczeństwa Inteligentnych sieci. W pierwszej kolejności należy oprzeć się na już wypracowanych standardach:

- ISO/IEC 62443 (ISA99),
- NIST 800-82,
- ISO/IEC 27001,
- COBIT,
- ITIL.

oraz uwzględnić kontekst i potrzebę:

- AMI System Security Specification,
- NIST 7628 Guidelines for Smart Grid Cybersecurity,
- Urząd Regulacji Energetyki Specyfikacja Techniczna na dostęp do infrastruktury licznikowej dla systemu AMI opracowanie opublikowane 25.03.2015 r.
- ENISA Smart Grid Security.

Standardy oraz doświadczenie wskazuje, że do osiągnięcia skuteczności w zakresie ochrony kluczowych zasobów, takich jak infrastruktura AMI

czy całość Smart Grid konieczna jest koncentracja na następujących obszarach:

- prawidłowym określeniu priorytetów i kluczowych zasobów (uwzględniając zarówno informacje, jak i kluczowe zasoby i technologie IT i OT (*Operational Technology*),
- świadomości pracowników,
- zabezpieczeniu wykorzystywanych technologii IT i OT,
- kontroli ryzyka w relacjach biznesowych (ze szczególnym uwzględnieniem dostawców),
- umiejętności monitorowania bezpieczeństwa i reakcji w sytuacji kryzysowej,
- budowy procesów i kompetencji pozwalających na właściwe szacowanie ryzyka.

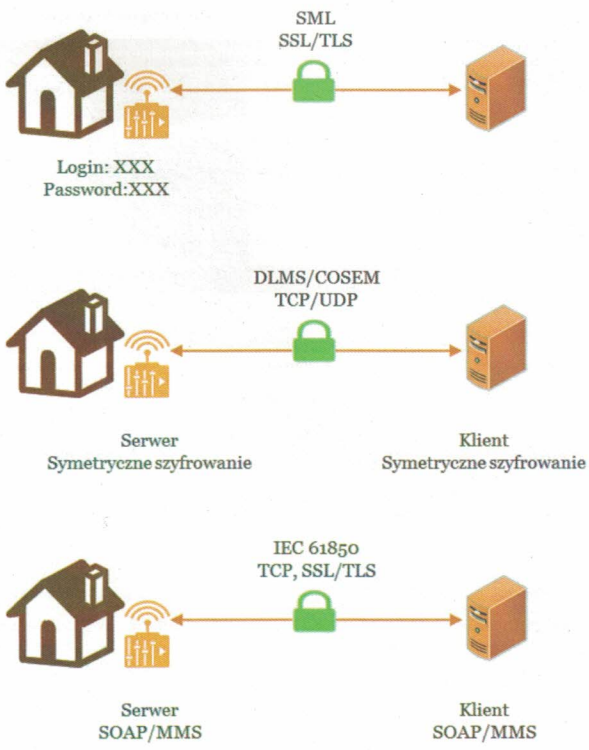
Pozwoli to skupić się na zbudowaniu jednolitych zasad dla:

- zarządzania dostępem do kluczowych zasobów sieci,
- uwierzytelnienia użytkowników oraz urządzeń funkcjonujących w sieci,
- szyfrowania danych,
- zasad zabezpieczenia przed DDoS (ang. *Distributed Denial of Service*, rozproszona odmowa usługi),
- zarządzania aktualizacjami oprogramowania urządzeń oraz systemów,
- architektury bezpieczeństwa systemu, integracji IT i automatyki przemysłowej,
- podnoszenia świadomości oraz szkolenia pracowników,
- budowania ciągłości działania i planów awaryjnych,
- łańcucha dostaw i współpracy z firmami wspierającymi pracę sieci,
- zarządzania użytkownikami uprzywilejowanymi.

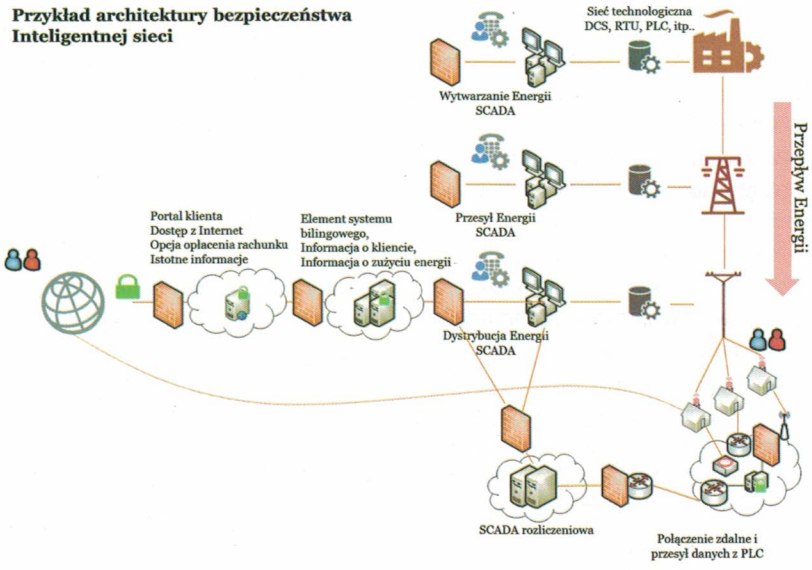
Zbudowanie spójnych reguł, z uwzględnieniem kontekstu, pozwoli na ograniczenie wpływu zagrożeń jak i ograniczy koszty w przypadku, gdy podejście do bezpieczeństwa ma charakter wyspowy.

Dla przykładu:

Zastosowanie Infrastruktury Klucza Publicznego (PKI) na potrzeby Inteligentnej sieci pozwala nam pośrednio i bezpośrednio zaadresować kwestie szyfrowania danych (transmisja) jak i kwestie związane z uwierzytelnieniem elementów infrastruktury.



Rys. 5. Proces uwierzytelnienia oraz szyfrowanie transmisji dla elementów Smart Grid



Rys. 6. Architektura bezpieczeństwa Inteligentnych sieci

Możliwe schematy wykorzystania przedstawiono na rys. 5.

Przykład kompleksowej architektury Inteligentnej sieci z uwzględnieniem kwestii bezpieczeństwa przedstawiono na rys. 6. Na rysunku użyto pojęcia

SCADA (ang. *Supervisory Control And Data Acquisition*) - system informatyczny nadzorujący przebieg procesu technologicznego lub produkcyjnego. Jego główne funkcje obejmują zbieranie aktualnych danych (pomiarów), ich wizualizację, sterowanie procesem, alarmowanie oraz archiwizację danych.

Całościowe podejście do bezpieczeństwa w kontekście projektowania architektury oraz procesów inteligentnych sieci pozwala nam na budowanie adekwatnego podejścia do bezpieczeństwa nowoczesnej sieci elektroenergetycznej. W kontekście funkcjonowania takiej sieci niezwykle ważna staje się potrzeba monitorowania zdarzeń i zbudowanie Security Operation Center (ang. *Centrum monitorowania i reagowania na zdarzenia bezpieczeństwa*). Dodatkowo należy zwrócić uwagę, że wprowadzenie AMI będzie oznaczało, że nasz dostawca energii będzie miał dostęp do nowego rodzaju danych - danych osobowych. Ich ochrona na tle innego rodzaju danych jest jedną z najbardziej restrykcyjnych i regulowanych w Europie. W przypadku AMI, danymi osobowymi będą wszystkie dane pozwalające charakteryzować lub profilować odbiorców, np. kiedy zwiększa/zmniejsza się pobór prądu (odbiorca jest w domu i korzysta z komputera lub telewizora). W związku z tym pobieranie, przechowywanie i udostępnianie danych pomiarowych traktowane jest jako przetwarzanie danych osobowych.

Prezes URE, dbając o poszanowanie praw odbiorców energii, podkreśla, że w świetle najnowszej nowelizacji Prawa energetycznego informacje pomiarowe uzyskiwane za pomocą inteligentnych liczników podlegają takiej samej ochronie jak dane osobowe. Zgodnie z art. 9 c ust. 5a ustawy z 10 kwietnia 1997 Prawo energetyczne: *Operatorzy systemów dystrybucyjnych instalujący u odbiorców końcowych przyłączonych do ich sieci liczniki zdalnego odczytu są obowiązani chronić dane pomiarowe dotyczące tych odbiorców, na zasadach określonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.)*

W związku z niedawnymi zmianami prawa europejskiego w tym zakresie, konieczne jest przyjrzenie się nowym regulacjom - przepisom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które mają zostać wdrożone w całej Unii Europejskiej do 25 maja 2018 r. Zgodnie z tymi regulacjami, operatorzy systemów dystrybucyjnych będą zobowiązani do wprowadzenia szeregu mechanizmów, do procesów/usług/systemów w ramach, których przetwarzane są dane osobowe, m.in.:

- *Privacy Impact Assessment* - ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych,
- *Privacy by Design* - uwzględnienie ochrony danych w fazie projektowania,
- *Privacy by Default* - domyślna ochrona danych,
- zgłaszanie naruszenia ochrony danych organowi nadzorczemu,
- obowiązek konsultacji z organem nadzoru (w wybranych przypadkach),
- określenie sposobu usuwania danych klienta (w tym z kopii zapasowych)
- nowe regulacje mogą prowadzić do konieczności usuwania danych wielu klientów codziennie.

> Nieupoważniona ingerencja w infrastrukturę przez cyberprzestępcę może doprowadzić do strat zarówno wynikających bezpośrednio, jak i pośrednio z braku zasilania u odbiorców. Złożoność sieci powoduje ryzyko istnienia luk, które jeszcze nie zostały zidentyfikowane

Warto wskazać, że branża energetyczna otrzymała już w 2012 r. zalecenia Komisji Europejskiej, które zawierały podobne wymagania odnośnie przetwarzania danych osobowych pozyskiwanych poprzez stosowanie AMI (Zalecenie Komisji z dnia 9 marca 2012 r. w sprawie przygotowań do rozpowszechnienia inteligentnych systemów pomiarowych). W zaleceniu tym przewidziane zostały zarówno oceny skutków planowanych operacji przetwarzania jak i uprzednie konsultacje z organem nadzoru, uwzględnienie danych w fazie projektowania i stosowanie domyślnej ochrony danych, a także stosowanie odpowiednich środków mających na celu bezpieczeństwo danych. Nowe rozporządzenie unijne czyni te zalecenia obowiązującym prawem, nie tylko w stosunku do danych osobowych pozyskiwanych wskutek stosowania AMI, ale także wszelkich innych danych osobowych przetwarzanych przez spółki sektora energetycznego.

Konkluzja jest jedna w przypadku inteligentnych sieci energetycznych, bezpieczeństwo jest jednym z istotniejszych aspektów dobrej implementacji. Tylko podejście całościowe, w którym każde ryzyko jest mierzone tą samą miarą i rozpatrywane pod różnymi aspektami, skutków jego materializacji pozwoli na skuteczną mityzację zagrożeń. □