Analiza zasadności ustanowienia sektorowego zespołu cyberbezpieczeństwa w sektorze energii. Wnioski i rekomendacje.

Wstęp

Dane na potrzeby opracowania zostały zebrane w czasie dedykowanych warsztatów, które odbyły się w dniu 12 i 14 grudnia 2018 r. w siedzibie Ministerstwa Energii w Warszawie. W warsztatach wzięli udział przedstawiciele przedsiębiorców z sektora energia, przedstawiciele Ministerstwa Energii.

Zgodnie z założeniami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej UoKSC) Ministerstwo Energii jako organ właściwy ds. cyberbezpieczeństwa może ustanowić sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora. Niniejszy raport ma stanowić wsparcie Ministra Energii w zakresie realizacji przepisów ustawy poprzez:

1. przygotowanie katalogu usług możliwych do świadczenia przez CSIRT sektorowy (sektor energia) w postaci podręcznika,
2. przygotowanie szczegółowego opisu obowiązku operatora usługi kluczowej – w tym wobec CSIRT wyższego poziomu w przełożeniu na usługi CSIRT wg FIRST CSIRT Services Framework 1.1,
3. zbadanie zapotrzebowania przedsiębiorców na usługi CSIRT w sektorze energia w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa we wszystkich podsektorach sektora,
4. zorganizowanie i przeprowadzenie warsztatów w siedzibie Ministerstwa Energii.
5. przygotowanie rekomendacji w zakresie utworzenia i struktury zespołu/zespołów CSIRT w ramach sektora energia.

Metodyka pracy

Określenie zapotrzebowania przedsiębiorców w sektorze energia (w rozumieniu UoKSC) na usługi CSIRT we wszystkich podsektorach sektora oraz preferencji podmiotów sektora do utworzenia sektorowego zespołu bezpieczeństwa zostały oparte o badania ankietowe.

W pierwszym etapie realizacji zamówienia opracowano ankiety dostosowane do sektora energia. Za podstawę w opracowaniu ankiet zespół przyjął wykaz usług świadczonych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego, zawarty w dokumencie pn. *FIRST CSIRT Framework – Computer Security Incident Response Team (CSIRT) Services Framework*. Dokument został opracowany przez Forum Zespołów Reagowania na Incydenty i Bezpieczeństwa (*Forum of Incident Response and Security Teams – FIRST*) na potrzeby standaryzacji usług świadczonych przez zrzeszone zespoły CSIRT i jest uznawany w środowisku CERT/CSIRT za podstawę ich pracy.

W kolejnym etapie zostały zorganizowane i przeprowadzane warsztaty w siedzibie Ministerstwa Energii. Warsztaty zostały podzielone na dwie części. W ramach wstępu uczestnicy zostali zapoznani z obowiązkami operatorów usług kluczowych oraz ze wszystkimi usługami zawartymi w dokumencie *FIRST CSIRT Framework – Computer Security Incident Response Team (CSIRT) Services Framework*. W drugiej części spotkania uczestnicy wypełnili ankiety. Wraz z danymi o strukturze sektora energia stały się podstawą do przygotowania wniosków i rekomendacji.

Katalog usług CSIRT oraz przypisanych im funkcji był przedmiotem badań ankietowych, którym poddano uczestników warsztatów przeprowadzonych w dniach 12 i 14 grudnia 2018 r. Badania dotyczyły czterech zagadnień:

1. oceny potrzeby ustanowienia CSIRT dla podsektorów,
2. oszacowania istotności danej usługi CSIRT dla zapewnienia cyberbezpieczeństwa,
3. określenia, które usługi powinny być świadczone przez CSIRT sektorowy,
4. określenia, kto powinien świadczyć usługi CSIRT sektorowego.

W ankiecie wzięło udział 85 osób. Bazując na strukturze organizacyjnej sektora energia oraz wynikach ankiet, zespół przygotował tabele i wykresy, które umożliwiły określenie, który podsektor reprezentowali uczestnicy oraz określenie istotności każdej z usług dla danego podsektora. Przedstawione zostały również

zapotrzebowanie na ustanowienie sektorowego CSIRT-u oraz rekomendacje, kto powinien świadczyć usługi CSIRT sektorowego i dla jakich usług.

Biorąc pod uwagę fakt, że 40% (34/85) ankietowanych zaznaczyło w odpowiedzi na pytanie 1 (Jaki podsektor (sektora Energia) Państwo reprezentują?), że reprezentuje więcej niż 1 podsektor, odpowiedzi te zostały rozłożone równomiernie pomiędzy każdy ze wskazanych podsektorów. Wynika to z faktu (co potwierdziły rozmowy po sesji pytań), iż podmiot reprezentujący więcej niż 1 podsektor nie rozdziela znaczenia usług i preferencji co do utworzenia CSIRT sektorowego, kierując się potrzebami podsektora, a potrzebami danego podmiotu. Dzieje się tak m.in. dlatego, że obowiązki wskazane w UoKSC będą realizowane w całym podmiocie (jednakowo) bez podziału na wykonywane rodzaje działalności (np. zostanie powołana jedna wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo, a nie oddzielne dla każdego rodzaju działalności).

Wnioskując zespól skupił się na najistotniejszych kwestiach związanych z potencjalnym utworzeniem sektorowego CSIRT-u, co w rezultacie zgodnie z założeniami umożliwiło przygotowanie rekomendacji dla Ministerstwa Energii w tym zakresie.

Poniżej przedstawiony został wykaz usług, które zawarte były w ankiecie:

1. OBSZAR USŁUGOWY – ZARZĄDZANIE INCYDENTAMI
    - U1 – OBSŁUGA INCYDENTU
    - U2 – ANALIZA INCYDENTU
    - U3 – NEUTRALIZACJA INCYDENTU I PRZYWRÓCENIE USŁUG
2. OBSZAR USŁUGOWY – ANALIZY
    - U4 – ANALIZA ARTEFAKTÓW
    - U5 – ANALIZA POWŁAMANIOWA (INFORMATYKA ŚLEDCZA)
    - U6 – ANALIZA PODATNOŚCI
3. OBSZAR USŁUGOWY – ZAPEWNIENIE BEZPIECZEŃSTWA INFORMACJI
    - U7 – SZACOWANIE RYZYKA
    - U8 – WSPARCIE DLA WYKORZYSTYWANYCH W ORGANIZACJI POLITYK

U9 – WSPARCIE DLA PLANOWANIA CIĄGŁOŚCI DZIAŁANIA I PRZYWRACANIA DO DZIAŁANIA PO AWARII

U10 – WSPARCIE TECHNICZNE DLA PROCESÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

U11 – ZARZĄDZANIE POPRAWKAMI

4. OBSZAR USŁUGOWY – ŚWIADOMOŚĆ SYTUACYJNA

U12 – DZIAŁANIA POMIAROWE

U13 – SYNTEZA I ANALIZA DANYCH

U14 – ROZWÓJ ORAZ ZARZĄDZANIE ŹRÓDŁAMI I DANYMI THREAT INTELLIGENCE

5. OBSZAR USŁUGOWY – KOMUNIKACJA

U15 – PODNOSZENIE ŚWIADOMOŚCI O ZAGROŻENIACH

U16 – DORADZTWO W ZAKRESIE POLITYK I STRATEGII CYBERBEZPIECZEŃSTWA

U17 – DZIELENIE SIĘ INFORMACJĄ I UPUBLICZNIANIE JEJ

6. OBSZAR USŁUGOWY – ROZWÓJ ZDOLNOŚCI

U18 – POMIAR POZIOMU ŚWIADCZENIA USŁUG

U19 – SZKOLENIA I EDUKACJA

U20 – ORGANIZACJA ĆWICZEŃ

U21 – DORADZTWO TECHNICZNE

U22 – GROMADZENIE I WYKORZYSTANIE NABYTYCH DOŚWIADCZEŃ

7. OBSZAR USŁUGOWY – BADANIA I ROZWÓJ

U23 – ROZWÓJ METODYK ZARZĄDZANIA PODATNOŚCIAMI

U24 – ROZWÓJ TECHNOLOGII I PROCESÓW THREAT INTELLIGENCE

U25 – ROZWÓJ WŁASNYCH NARZĘDZI CYBERBEZPIECZEŃSTWA

Tabela 1 Podsektory sektora energia

	PODSEKTORY SEKTORA ENERGIA	SUMA ODPOWIEDZI
1.	WYDOBYWANIE KOPALIN	16
2.	ENERGIA ELEKTRYCZNA	37
3.	CIEPŁO	50
4.	ROPA NAFTOWA	4
5.	GAZ	11
6.	DOSTAWY I USŁUGI DLA SEKTORA ENERGII	16
7.	JEDNOSTKI NADZOROWANE I PODLEGŁE	12

PODMIOTY ŚWIADCZĄCE USŁUGI CSIRT SEKTOROWEGO

W odpowiedziach na kolejne pytanie uwzględniono sześć podmiotów, które mogłyby świadczyć usługi CSIRT sektorowego dla sektora energia. Każdy z uczestników mógł zaznaczyć jedną odpowiedź. W dyskusji przeprowadzonej podczas warsztatów uczestnicy zasygnalizowali swoją wątpliwość co do tego, kto powinien świadczyć usługi CSIRT-u sektorowego. W wyniku tego zespół dopisał siódmą odpowiedź o treści „nie wiem". Odpowiedzi respondentów zostały zsumowane i przedstawione w postaci wartości procentowej na wykresie poniżej (podmioty w tabeli są numerowane kolejno analogicznie jak w przypadku ankiet).

WNIOSKI Z ANALIZY DANYCH

1. Usługi CSIRT są istotne dla zapewnienia bezpieczeństwa usług kluczowych w sektorze energia. Jest to wyrażone wysoką średnią ocen w odpowiedziach na pytanie 2., które brzmiało: „Jak dana usługa CSIRT jest istotna dla zapewnienia bezpieczeństwa świadczonej przez Państwa usługi kluczowej?". W szczególny sposób dotyczy to usług operacyjnego reagowania na incydenty, w tym wykonywania specjalistycznych analiz technicznych oraz usług dotyczących budowania świadomości, w szczególności poprzez formy aktywne takie jak ćwiczenia czy szkolenia.
2. Podmioty w sposób zdecydowany oczekują wsparcia w realizacji usług „miękkich" związanych z budową świadomości, doradztwem w zakresie zagadnień organizacyjnych i technicznych oraz wsparciem w wypracowywaniu i wdrażaniu najlepszych praktyk. W mniejszym stopniu zaś oczekują wsparcia w realizacji usług operacyjnych, związanych z reagowaniem na incydenty (za wyjątkiem podwyższonego oczekiwania na świadczenie dla nich usług analitycznych U4, U5, U6). Najprawdopodobniej jest to wynik realnej oceny sytuacji związanej z poczuciem odpowiedzialności za skuteczne rozwiązanie incydentu po własnej stronie.
3. W podsektorze ropy naftowej poziom istotności danych usług, podobnie jak potrzeba realizacji usług przez CSIRT sektorowy oceniana jest wyraźnie niżej niż średnia dla sektora. Dotyczy to w praktyce wszystkich usług. Wynika to z reprezentowania tego podsektora przez małą liczbę podmiotów o wysokich własnych zdolnościach w obszarze Cyberbezpieczeństwa np. PKN Orlen SA czy PERN SA.
4. Odwrotna niż w sektorze ropy jest sytuacja w podsektorze gazu i wśród jednostek nadzorowanych i podległych. W tych przypadkach ocena istotności usług CSIRT-owych jest na wyraźnie wyższym poziomie.
5. Najmniejsza skłonność do delegacji usług CSIRT-owych do sektorowego zespołu cyberbezpieczeństwa jest w podsektorach: wydobywanie kopalin, energii elektrycznej, ropy naftowej oraz dostawy i usług (w przypadku usług o charakterze operacyjnym).
6. Są dwa główne podmioty wskazywane jako potencjalny organizator zespołu CSIRT: Ministerstwo Energii oraz zdefiniowany jako spółka celowa powołana do pełnienia funkcji CSIRT-u sektorowego.
7. Po przeanalizowaniu ankiet uznano, że nie ma uzasadnienia do tworzenia CSIRT dla poszczególnych podsektorów. Wyniki nie są determinowane reprezentowanym podsektorem, a poziomem dojrzałości ankietowanych organizacji do reagowania na incydenty komputerowe, co jest związane zarówno z wielkością podmiotu i zasobami, którymi dysponuje w tym obszarze. Warto zauważyć bowiem, że wśród

zaproszonych do udziału w warsztatach organizacji, podmioty małe były reprezentowane właściwie tylko w podsektorze ciepło.

8. Usługi wskazywane jako preferowane do świadczenia przez potencjalny CSIRT sektorowy (średnia powyżej 3,0) znajdują się w 14 obszarach usługowych (U4, U5, U6, U14, U15, U16, U17, U19, U20, U21, U22, U23, U24, U25). Wskazanie grupy usług z obszaru „Zarządzanie incydentami" może oznaczać aktualny brak samodzielnych zdolności niektórych podmiotów sektora (nadreprezentacja w podsektorze ciepło wynika ponownie z faktu najmniejszej dojrzałości podmiotów tego podsektora do reagowania na incydenty komputerowe. Usługi typowane przez ankietowanych odpowiadają usługom świadczonym przez zespoły CSIRT na świecie. Zasadniczo usługi świadczone przez zespoły CSIRT można podzielić na cztery grupy usług:

   - Usługi reagowania i analizy incydentów (U1, U2, U3)
   - Dostarczanie najbardziej zaawansowanych analiz (U4, U5, U6).
   - Usługi w obszarze „Świadomość sytuacyjna" związane z cyber threat intelligence (U12, U13 i U14).
   - Usługi badawczo-rozwojowe (U23, U24, U25).

REKOMENDACJE

1. Należy powołać jeden CSIRT sektorowy świadczący usługi w zakresie:
    - Dostarczania najbardziej zaawansowanych analiz (U4, U5, U6).
    - Usług cyber threat intelligence (U12, U13 i U14).
    - Usług badawczo-rozwojowych (U23, U24, U25).
    - Dzielenie się wiedzą z podmiotami sektora oraz rozwój zdolności (U15, U19, U20).
2. CSIRT sektorowy powinien mieć zdolność do świadczenia ww. usług w obszarze automatyki przemysłowej.
3. W przypadku uznania za operatorów usług kluczowych dużej liczby małych podmiotów CSIRT sektorowy powinien mieć zdolność do wspierania ich również w zakresie usług z pozostałych obszarów, w tym w szczególności operacyjnego reagowania na incydenty U1, U2, U3 oraz usług U10 i U11.
4. Pomimo wskazania przez większość ankietowanych (31%) spółki celowej jako formy organizacji CSIRT sektorowego, w praktyce jest to rozwiązanie trudne w realizacji, zwłaszcza w przypadku dużej liczebności zainteresowanych podmiotów oraz różnicy poziomów dojrzałości do reagowania na incydenty komputerowe (konieczne uzgodnienia statutu ze wszystkimi interesariuszami). W związku z tym, jako rozwiązanie optymalne, rekomenduje się powołanie sektorowego zespołu CSIRT w najlepiej przygotowanym do tego podmiocie. Potencjalnymi kandydatami są: PSE SA, OPG Gaz-System SA oraz PGE SA.
5. Wypracować zdolność do świadczenia części usług CSIRT-owych w Ministerstwie Energii. Zdolności te, dotyczyłyby:
    - prowadzenia działań uświadamiających (U15, U17),
    - szkoleń i ćwiczeń (U19 i U20),
    - doradztwa organizacyjno-procesowego (U16)
    - oraz stałego monitoringu jakości funkcjonowania wszystkich usług CSIRT-owych w sektorze energii (U18).