Opis CSIRT dla CERT Energa

1. O tym dokumencie
   1.1. Data ostatniej aktualizacji

   To jest wersja 1.0, opublikowana dnia 22 lipca 2019 r.

   1.2. Lista dystrybucyjna dla powiadomień

   Obecnie CERT Energa nie używa list dystrybucyjnych do powiadamiania o zmianach w tym dokumencie.

   1.3. Lokalizacje, w których można znaleźć ten dokument

   Aktualna wersja tego opisu CSIRT jest dostępna na stronie internetowej CERT Energa. Jego adres URL to https://cert.energa.pl/kontakt
2. Informacje kontaktowe
   2.1. Skrócona nazwa zespołu

   CERT Energa

   2.2. Nazwa zespołu

   Computer Emergency Response Team Energa

   2.3. Adres

   CERT Energa

   Energa Informatyka i Technologie sp. z o.o.

   Aleja Grunwaldzka 472A

   80-309 Gdańsk

   Polska

   2.4. Strefa czasowa

   Czas środkowoeuropejski (GMT+0100, GMT+0200 od kwietnia do października)

   2.5. Numer telefonu

   Telefon stacjonarny: +48 58 527 91 11

   2.6. Numer faksu

   Brak dostępu

   2.7. Adres mailowy

   cert@energa.pl

   2.8. Klucze publiczne i inne informacje o szyfrowaniu

   Aktualnie niedostępny

2.9. Inne informacje

Ogólne informacje o CERT Energa, a także linki do różnych zalecanych zasobów bezpieczeństwa, można znaleźć na stronie https://cert.energa.pl/

2.10. Punkty kontaktu z Klientem

Preferowaną metodą kontaktu z CERT Energa jest e-mail na adres cert@energa.pl
E-mail wysłany na ten adres będzie obsługiwany przez odpowiedzialnego człowieka.

Jeśli korzystanie z poczty elektronicznej nie jest możliwe (lub nie jest wskazane ze względów bezpieczeństwa), z CERT Energa można skontaktować się telefonicznie przez całą dobę.

Godziny pracy CERT Energa są zwykle ograniczone do zwykłych godzin pracy (08:00 - 16:00 CET / CEST od poniedziałku do piątku z wyjątkiem świąt) z całodobowym dyżurem.

3. Statut

3.1. Opis misji

Główną rolą CERT Energa jest obsługa operacyjna globalnych incydentów bezpieczeństwa teleinformatycznego z wczesnym ostrzeganiem, wykrywaniem zagrożeń, analizą złośliwego oprogramowania, wydawaniem komunikatów bezpieczeństwa, ocenami bezpieczeństwa i audytami, a także konsultacjami w dziedzinie bezpieczeństwa IT.

3.2. Domena

Domena CERT Energa to:

- ASN: 28689

- IP: 91.208.150.0/24 and 91.209.155.0/24;

- Domeny: actaenergetica.org, cieplokaliskie.com.pl, e-elektrownie.pl, elektrowniaostroleka.pl, energa-finance.se, energa-kogeneracja.pl, energa-operator.pl, energa-slovakia.sk, energa.pl, energaathleticcup.pl, energabasketcup.pl, energasailing.pl, energasport.pl, energawisla.pl, partnerenerga.pl, planetaenergii.pl, salonenerga.pl, swiecsie.pl

3.3. Sponsoring i/lub Przynależność

CERT Energa jest finansowo utrzymywany przez Grupę Energa, której formalnie jest częścią.

3.4. Autorytet

CERT Energa działa pod patronatem i pod nadzorem delegowanym przez Energa S.A.

CERT Energa oczekuje współpracy z administratorami systemu i użytkownikami (Klientami) w sieci Grupy Energa. Jednakże, jeśli uzasadniają to okoliczności, CERT Energa jest uprawniony do podjęcia środków, które uzna za właściwe, aby odpowiednio obsłużyć incydent związany z bezpieczeństwem informacji.

4. Polityki

4.1. Rodzaje incydentów i poziom wsparcia

CERT Energa jest upoważniona do reagowania na wszelkiego rodzaju incydenty związane z bezpieczeństwem informacji, które występują lub mogą wystąpić w sieciach Grupy Energa.

Poziom wsparcia udzielanego przez CERT Energa będzie się różnić w zależności od rodzaju i wagi incydentu lub problemu, rodzaju elementu, ilości użytkowników, której dotyczy problem, oraz zasobów CERT Energa w tym czasie.

Zdarzenia będą traktowane priorytetowo według wagi i ważności.

4.2. Współpraca, interakcja i ujawnianie informacji

CERT Energa wymienia wszystkie niezbędne informacje z innymi zespołami CSIRT, a także z administratorami zainteresowanych stron. Żadne dane osobowe lub inne dane ogólne nie są wymieniane, chyba że wyraźnie to wskazano.

Wszystkie wrażliwe dane (takie jak dane osobowe, konfiguracje systemu, znane luki w zabezpieczeniach związane z ich lokalizacjami) są szyfrowane, jeśli muszą zostać przesłane przez niezabezpieczone środowisko.

4.3. Komunikacja i uwierzytelnianie

Nieszyfrowane wiadomości e-mail nie będą uważane za szczególnie bezpieczne, ale wystarczą do transmisji danych o niskiej czułości. Jeśli konieczne będzie przesłanie bardzo wrażliwych danych pocztą e-mail, zostanie użyta GPG. Sieciowe transfery plików zostaną uznane za podobne do poczty elektronicznej do tych celów: wrażliwe dane powinny być szyfrowane w celu transmisji.

5. Usługi

5.1. Reagowanie na incydenty

CERT Energa pomoże administratorom systemu w obsłudze technicznych i organizacyjnych aspektów incydentów. W szczególności zapewni pomoc lub poradę w odniesieniu do następujących aspektów zarządzania incydentami:

5.1.1. Analiza incydentu

- Badanie, czy rzeczywiście miał miejsce incydent,
- Określenie zakresu incydentu.

5.1.2. Koordynacja incydentów

- Ustalenie pierwotnej przyczyny incydentu (wykorzystana luka),
- Ułatwienie kontaktu z innymi stronami, które mogą być zaangażowane,
- W razie potrzeby ułatwianie kontaktu z odpowiednimi funkcjonariuszami organów ścigania,
- Robienie raportów do innych zespołów CSIRT,
- Redagowanie ogłoszeń dla użytkowników, jeśli dotyczy.

5.1.3. Rozwiązywanie incydentów

CERT Energa udziela porad, ale nie zapewnia fizycznego wsparcia klientom z wewnętrznej sieci Grupy Energa w zakresie rozwiązywania incydentów.

- Usunięcie podatności.
- Zabezpieczenie systemu przed skutkami incydentu.
- Zbieranie dowodów zdarzenia.

Ponadto CERT Energa będzie gromadzić statystyki dotyczące przetwarzanych incydentów i powiadomi społeczność w razie potrzeby, aby pomóc jej w ochronie przed znanymi atakami.

5.2. Usługi proaktywne

CERT Energa koordynuje i utrzymuje następujące usługi w możliwym zakresie, w zależności od zasobów:

- Usługi informacyjne za pośrednictwem następujących kanałów:
- strona internetowa: https://cert.energa.pl/
- Usługi szkoleniowe i edukacyjne

6. Formularze zgłaszania incydentów

CERT Energa obsługuje tylko incydenty zgłoszone e-mailem lub telefonicznie. Dane kontaktowe są dostępne na stronie: https://cert.energa.pl/kontakt/

7. Zastrzeżenia

   Przy przygotowywaniu informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności. W związku z tym CERT Energa nie ponosi żadnej odpowiedzialności za błędy lub pominięcia, ani za szkody wynikające z wykorzystania informacji zawartych w raporcie.