

PGE Systemy powołały PGE-CERT, zespół reagowania na incydenty komputerowe.

PGE Systemy powołały PGE-CERT, zespół reagowania na incydenty komputerowe.

Główne zadania PGE-CERT:

- Reagowanie oraz kompleksowa obsługa incydentów bezpieczeństwa teleinformatycznego w Grupie Kapitałowej PGE.
- Minimalizacja skutków wystąpienia incydentów bezpieczeństwa teleinformatycznego.
- Komunikacja z właściwymi podmiotami oraz koordynowanie działań pomiędzy departamentami utrzymania oraz spółkami w ramach rozwiązywania incydentów bezpieczeństwa teleinformatycznego.
- Współpraca z instytucjami oraz służbami i organami państwowymi odpowiedzialnymi za bezpieczeństwo teleinformatyczne.
- Komunikacja z zespołami CSIRT/CERT w zakresie alarmowania, obsługiwania oraz ograniczania ryzyk w związku z incydentami bezpieczeństwa teleinformatycznego.
- Monitorowanie bezpieczeństwa usług dla podmiotów Grupy PGE.

Traffic Light Protocol

Podobnie jak inne zespoły cyberbezpieczeństwa, PGE-CERT używa protokołu Traffic Light Protocol (TLP). Protokół został stworzony w celu kontrolowania i zachęcania do dzielenia się informacjami.

Co to jest TLP?

Traffic Light Protocol jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

TLP:RED Informacje przeznaczone wyłącznie dla bezpośrednich odbiorców

TLP:AMBER Informacje przeznaczone dla pracowników organizacji

TLP:GREEN Informacje przeznaczone dla całego sektora, bez publikowania w sieci Internet

TLP:WHITE Informacje przeznaczone dla wszystkich. Nie podlegające żadnym ograniczeniom (z wyjątkiem praw autorskich)

Informację o użytym TLP umieszczamy w nagłówku lub stopce przekazywanej wiadomości, przeważnie stosując zapis w formie: „TLP: [Kolor]”. Traffic Light Protocol nie ma zastosowania do informacji tajnych lub poufnych.

W przypadku kontaktu z PGE-CERT prosimy o oznaczenie informacji zgodnie z regułami TLP. Oznaczona przez TLP korespondencja powinna wskazywać kolor w temacie oraz w treści wiadomości e-mail, bezpośrednio przed samą określoną informacją.

Kolor TLP należy oznaczać dużymi literami: TLP: RED, TLP: AMBER, TLP: GREEN lub TLP: WHITE

Dane kontaktowe PGE-CERT

W nagłych wypadkach lub w sytuacjach kryzysowych skontaktuj się z PGE-CERT e-mailem, wysyłając wiadomość na adres

PGE Systemy S.A.

PGE-CERT, ul. Mysia 2, 00-496 Warszawa

Telefon alarmowy : +48 885 552 646; e-mail:

Prosimy o zawarcie w zgłoszeniu następujących informacji:

- dane kontaktowe i informacje organizacyjne
- imię i nazwisko oraz nazwa i adres organizacji
- adres e-mail
- numer telefonu
- adres(y) IP, FQDN(y) i każdy inny odpowiedni element techniczny wraz z powiązaną obserwacją
- wyniki skanowania (jeśli są) i /lub dowolny wycinek logów pokazujący problem

W celu zachowania poufności przesyłanych danych w kontaktach z PGE-CERT prosimy korzystać systemu PGP/GPG.

Nasz klucz GnuPG publiczny PGP:

- [Klucz GnuPG](#)

Opis zespołu PGE-CERT zgodny z RFC 2350

- [RFC 2350](#)

[Authorized Users of the CERT Mark >](#)



Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University