

SYSTEMY ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA I BEZPIECZEŃSTWO ENERGETYCZNE



ADAM GOREŃ

Koordynator Zespołu
Certyfikacji Systemów
Zarządzania
Departament Certyfikacji
i Oceny Zgodności
Urząd Dozoru Technicznego

Dostawy energii, wody, żywności mają fundamentalne znaczenia dla społeczeństwa, a ich bezpieczeństwo jest jednym z elementów charakteryzujących kraje wysoko rozwinięte. Przewidywanie zagrożeń i działania podejmowane w celu minimalizowania ich niekorzystnych skutków stanowią fundament zarządzania infrastrukturą krytyczną.

KLUCZOWA INFRASTRUKTURA

Niezakłócone dostawy energii i bezpieczeństwo energetyczne Polski są szczególnie istotne dla funkcjonowania gospodarki. Dostęp do pierwotnych nośników energii w tym gazu, węgla i ropy naftowej, ich transport i magazynowanie ma zasadniczy charakter, również z tego powodu, że dla pozostałych sektorów stanowi podstawowy czynnik umożliwiający ciągłość działania.

Inwestycje poczynione w ostatnich latach w zakresie infrastruktury umożliwiającej dywersyfikację dostaw gazu, w tym Terminal LNG, Baltic Pipe, rozbudowa sieci gazociągów oraz budowa nowych rurociągów i zbiorników magazynowych ropy naftowej i paliw płynnych jest działaniem, które mają znaczenie fundamentalne.

Wojna prowadzona na terenie państwa sąsiadującego z Polską powoduje znaczący wzrost ryzyka zmaterializowania się zagrożeń mogących wpłynąć na funkcjonowanie kluczowych elementów infrastruktury, w tym wspomnianej infrastruktury energetycznej.

Wprowadzony na terytorium całego kraju trzeci stopień alarmowy CRP (*Charlie-CRP*) dotyczący bezpieczeństwa w cyberprzestrzeni stanowi wymóg dla administracji publicznej oraz operatorów infrastruktury krytycznej zachowania szczególnej czujności w zakresie wystąpienia cyberzagrożeń.

Stopień Charlie-CRP wymusza na administracji publicznej oraz operatorach IK takie działania jak m.in. konieczność zapewnienia dostępności kluczowego personelu niezbędnego do funkcjonowania danej organizacji, przegląd zasobów, w tym zasobów, na wypadek konieczności ich wykorzystania, przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku.

KLUCZOWY PERSONEL

Zastępowalność kluczowych kadr zawsze stanowiła dla wielu organizacji wyzwanie. Zapewnienie stałej dostępności osób posiadających newralgiczną wiedzę umożliwiającą niezakłócone funkcjonowanie organizacji, osób posiadających odpowiednie kwalifikacje oraz uprawnienia z powodu sytuacji na rynku pracy, w tym demografii oraz potrzeb polskiej gospodarki, gdzie o te same zasoby rywalizuje między sobą szereg sektorów gospodarki jest obiektywnie trudne.

Organizacje, żeby sprostać tym wymaganiom muszą swoje działania na tym kierunku prowadzić z dużym wyprzedzeniem, działania te obejmują podnoszenie kompetencji własnych pracowników, modyfikacje procedur czy automatyzacje procesów.

Równolegle do wprowadzonego stopnia alarmowego Charlie-CRP Rządowe Centrum Bezpieczeństwa wydało rekomendacje **operatorom infrastruktury krytycznej** obejmujące działania, takie jak:

przegląd i aktualizację procedur bezpieczeństwa (w szczególności bezpieczeństwa teleinformatycznego, fizycznego, osobowego i technicznego),

przegląd procedur na wypadek zmaterializowania się zagrożeń kinetycznych, w tym o charakterze terrorystycznym,

przegląd i aktualizację planów ciągłości działania z uwzględnieniem zapasowego miejsca pracy czy też sprawdzenie działania środków łączności stosowanych w celu zapewnienia bezpieczeństwa.

KLUCZOWE DZIAŁANIA Z UDT

W UDT od lat promujemy wśród naszych partnerów podejście systemowe do wyzwań w zakresie zapewnienia ciągłości działania stojących przed operatorami infrastruktury krytycznej. Zarówno kierownictwo, jak i pracownicy powinni mieć świadomość i wiedzę nt. zagrożeń, obszarów ich występowania i wzajemnych powiązań oraz możliwości podejmowania działań prewencyjnych, poprawiając tym samym kulturę bezpieczeństwa.

Standard ISO 22301 stanowi ramę do identyfikacji kluczowych czynników ryzyka mających wpływ na organizację oraz na utrzymanie jej działań w najtrudniejszych warunkach.

Przeznaczona jest dla wszystkich organizacji, które chcą:

- doskonalić mechanizmy umożliwiające odtworzenie zdolności organizacji do ponownego działania w określonym czasie i na ustalonym poziomie w przypadku nieplanowanych zdarzeń,
- podnieść wiarygodność w oczach interesariuszy,
- zwiększyć konkurencyjność na rynku ze względu na zdolność do funkcjonowania niezależnie od niekorzystnych czynników,
- umożliwić skuteczną reakcję na sytuacje kryzysowe,
- poprawić wizerunek organizacji jako przygotowanej na nieprzewidziane zdarzenia.

Norma ISO 22301 może stanowić dobry punkt odniesienia dla wszystkich przedsiębiorstw, nie tylko operatorów infrastruktury krytycznej czy usług kluczowych, podejmujących prace służące określeniu środków, które mają zmniejszyć prawdopodobieństwo wystąpienia zakłóceń, skrócić czas ich trwania oraz ograniczyć ich wpływ na kluczowe produkty i usługi organizacji.

