Kategoria: Aktualności
Opublikowano: wtorek, 04, luty 2025 15:50
Odsłony: 1370

Cyberbezpieczeństwo w jednostkach administracji publicznej jest kluczowe dla zapewnienia stabilności, bezpieczeństwa i dobrobytu społeczeństwa. Bezpieczny sektor publiczny stanowi fundament obrony, ochrony danych oraz efektywnego dostępu do najważniejszych usług publicznych.

Zgodnie z Dyrektywą NIS2, zaniechanie obowiązków w zakresie cyberbezpieczeństwa może prowadzić do poważnych konsekwencji, zarówno prawnych, jak i operacyjnych. W przypadku podmiotów kluczowych, takich jak jednostki administracji publicznej, za niewypełnienie obowiązków nałożona może zostać kara w wysokości do 10 milionów euro lub 2% przychodów z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Dla podmiotów ważnych kara ta może wynieść do 7 milionów euro lub 1,4% przychodu. Dodatkowo, kara nie może być niższa niż 20 000 złotych w przypadku podmiotu kluczowego i 15 000 złotych w przypadku ważnego.

Oprócz sankcji finansowych, niedopełnienie obowiązków w zakresie cyberbezpieczeństwa może prowadzić do utraty zaufania obywateli do instytucji publicznych, co negatywnie wpływa na efektywność świadczenia usług publicznych. Dodatkowo, może to prowadzić do poważnych incydentów bezpieczeństwa, takich jak kradzież danych osobowych czy ataki na infrastrukturę krytyczną, co z kolei może mieć poważne konsekwencje dla bezpieczeństwa publicznego.

W związku z powyższym, jednostki administracji publicznej powinny traktować cyberbezpieczeństwo jako priorytet, wdrażając odpowiednie środki ochrony, monitorowania oraz reagowania na incydenty, aby zapewnić bezpieczeństwo danych i usług publicznych.

Dyrektywa NIS2 – nowe obowiązki dla instytucji publicznych

Wkrótce wejdzie w życie nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, mająca na celu implementację unijnej dyrektywy NIS2. Projekt nowelizacji znajduje się obecnie na etapie prac rządowych, a jego uchwalenie przez Sejm planowane jest w pierwszym kwartale 2025 roku.

Zgodnie z wymaganiami NIS2, instytucje muszą zapewnić ciągłe monitorowanie i reagowanie na incydenty bezpieczeństwa. Nałożony przy tym dość rygorystyczne terminy związane z powiadomieniem o incydencie:

- bezzwłocznie (max. 24 h) – wczesne ostrzeżenie ze wskazaniem, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub czy mógł wywrzeć wpływ transgraniczny;
- bezzwłocznie (max. 72 h) – zgłoszenie incydentu z ewentualną aktualizacją powyższych informacji, i wskazaniem wstępnej oceny poważnego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także wskaźników integralności systemu; dostawca usług zaufania dokonuje zgłoszenia w ciągu 24 godzin.

Aby zapewnić szybką identyfikacje i możliwość przekazania pełnych informacji o incydencie do CRSIT każdy urząd musi być przygotowany pod katem narzędzi, procedur i zespołów odpowiedzialnych za zarządzanie incydentami.

Wdrożenie SOC (Security Operation Center) stanowi efektywne rozwiązanie umożliwiające spełnienie tych wymogów, ponieważ zapewnia stałe monitorowanie infrastruktury IT, identyfikację zagrożeń oraz szybkie reagowanie na incydenty.

SOC składa się z 3 elementów:

- odpowiednio wykfalifikowanych osób w szeroką wiedzą o cyberbezpieczeństwie
- technologii niezbędnej do monitorowania i klasyfikacji zagrożeń np. narzędzia klasy SIEM, EDR, NDR/XDR
- procesów – określonych zadań jakie należy realizować aby zapobiegać incydentom oraz w przypadku ich pojawienia – szybko sobie z nimi poradzić

Ponieważ systemy informatyczne pracują w trybie ciągłym konieczne jest aby SOC, działał w trybie 24/7. Implementacja SOC pozwala na spełnienie tego wymogu poprzez zapewnienie ciągłego monitorowania i analizy zdarzeń bezpieczeństwa.

Warto zauważyć, że choć NIS2 nie nakłada bezpośredniego obowiązku posiadania SOC, bez takiej usługi trudno spełnić wymagania co do czasu analizy i zgłoszenia incydentu.

Security Operations Center (SOC)/ Szybka identyfikacja I eliminacja zagrożeń

Security Operations Center jest kompleksową usługą ciągłego monitorowania infrastruktury teleinformatycznej. Celem usługi jest wykrycie zagrożenia oraz podjęcie działania w celu jego wyeliminowania. Usługa realizowana jest w oparciu o trzy kluczowe komponenty – kapitał ludzki, technologię i procesy.

W nomenklaturze wojskowej Security Operations Center porównywany jest z jednostkami szybkiego reagowania. W praktyce usługa jest centrum zarządzania bezpieczeństwem cybernetycznym, realizując incydent response jako jeden z priorytetowych procesów.

Wszystkie kwestie poruszone w niniejszym artykule będą szerzej rozpatrywane na najbliższym webinarze organizowanym przez Blue energy – Operatora Security Operations Center (SOC).

“SOC dla Jednostek Administracji Samorządowej”

Udział w webinarium jest bezpłatny, a jego program został przygotowany z myślą o osobach odpowiedzialnych za optymalizację procesów związanych z obsługą incydentów bezpieczeństwa w administracji samorządowej.

- termin: **20 lutego 2025** (czwartek)
- godzina: **10:00 – 12:00**
- **rejestracja**.