IN.SE.CON 2026: cyberbezpieczeństwo państwa, miast i instytucji publicznych tematem debat w Poznaniu

Kategoria: Aktualności
Opublikowano: wtorek, 10, marzec 2026 11:46
Joanna Gryboś-Chechelska

Cyberataki na instytucje publiczne, rosnące znaczenie infrastruktury krytycznej oraz nowe regulacje w obszarze cyberbezpieczeństwa sprawiają, że temat odporności cyfrowej staje się jednym z kluczowych wyzwań także dla samorządów. O najważniejszych trendach, zagrożeniach i rozwiązaniach w tym obszarze będą dyskutować uczestnicy IN.SE.CON 2026 – Międzynarodowy Kongres Cyberbezpieczeństwa i Technologii Przełomowych, który odbędzie się 15–16 kwietnia br. w Poznaniu.

Wydarzenie współorganizowane przez Ministerstwo Obrony Narodowej oraz Grupa MTP zgromadzi przedstawicieli administracji publicznej, wojska, biznesu oraz środowiska eksperckiego. Program kongresu realizowany będzie na trzech równoległych scenach odpowiadających na potrzeby decydentów, kadry zarządzającej oraz specjalistów operacyjnych.

Scena Główna – strategiczna perspektywa bezpieczeństwa państwa

Scena Główna kongresu będzie przestrzenią debat strategicznych dotyczących bezpieczeństwa państwa w erze cyfrowej. W dyskusjach udział wezmą przedstawiciele administracji rządowej, dowództwa wojskowego, instytucji międzynarodowych oraz eksperci nowych technologii.

W programie zaplanowano wystąpienia m.in. Krzysztofa Gawkowskiego – Ministra Cyfryzacji oraz Cezarego Tomczyka, Sekretarza Stanu w Ministerstwie Obrony Narodowej. Uczestnicy debat będą rozmawiać m.in. o roli technologii przełomowych w nowym typie konfliktów XXI wieku oraz o potencjale Polski w rozwijaniu technologii przyszłości.

Dla przedstawicieli administracji lokalnej szczególnie istotny będzie kontekst bezpieczeństwa infrastruktury publicznej oraz odporności państwa na zagrożenia cyfrowe. Dyskusje na scenie głównej pokażą, w jaki sposób rozwój technologii – takich jak sztuczna inteligencja, systemy autonomiczne czy nowe sieci komunikacyjne – wpływa na funkcjonowanie instytucji publicznych, infrastruktury miejskiej oraz usług świadczonych mieszkańcom.

Debaty te pozwolą lepiej zrozumieć strategiczne kierunki polityki państwa w obszarze cyberbezpieczeństwa, które w najbliższych latach będą miały bezpośredni wpływ także na funkcjonowanie jednostek samorządu terytorialnego.

Scena Biznesu i Samorządu – praktyczne wyzwania cyberbezpieczeństwa w administracji lokalnej

Jednym z najważniejszych elementów programu dla przedstawicieli administracji lokalnej będzie Scena Biznesu i Samorządu, przygotowana z myślą o osobach zarządzających instytucjami publicznymi, operatorach infrastruktury krytycznej oraz kadrze menedżerskiej.

Program tej części kongresu koncentruje się na praktycznych aspektach budowania odporności cybernetycznej organizacji oraz dostosowywania się do nowych wymagań regulacyjnych. Wśród kluczowych tematów znajdą się m.in.:

- wyzwania związane z wdrażaniem dyrektyw NIS2 i CER,
- funkcjonowanie sektorowych modeli współpracy ISAC, umożliwiających wymianę informacji o zagrożeniach między instytucjami i operatorami infrastruktury,
- budowanie kultury cyberbezpieczeństwa w organizacji, w tym skuteczne szkolenie pracowników i ograniczanie ryzyka incydentów wynikających z błędów ludzkich.

Szczególna uwaga poświęcona zostanie również zagadnieniu cyberodporności miast i infrastruktury komunalnej. W kontekście rosnącej liczby systemów cyfrowych wykorzystywanych w zarządzaniu transportem, energią czy gospodarką wodną bezpieczeństwo tych rozwiązań staje się jednym z kluczowych elementów stabilnego funkcjonowania samorządów. Eksperci przedstawią także nowe podejścia do edukacji pracowników administracji, w tym wykorzystanie technologii VR w szkoleniach z zakresu cyberbezpieczeństwa, które pozwalają symulować realistyczne scenariusze incydentów. W programie znajdą się również wystąpienia dotyczące zarządzania ryzykiem związanym z wykorzystaniem sztucznej inteligencji w organizacjach, w tym zagrożeń takich jak prompt injection, manipulacja treścią generowaną przez modele AI czy wycieki danych.

Scena Profesjonalistów – wiedza dla zespołów IT i bezpieczeństwa

Program kongresu uzupełnia Scena Profesjonalistów, skierowana do praktyków cyberbezpieczeństwa – zespołów SOC, CSIRT, CERT, analityków zagrożeń oraz specjalistów odpowiedzialnych za ochronę systemów IT.
Program obejmuje trzy bloki tematyczne: prewencję, aktywną obronę oraz zarządzanie kryzysowe. Wśród poruszanych zagadnień znajdą się m.in. analiza pełnego łańcucha ataku w środowiskach IoT, wykorzystanie frameworku MITRE ATT&CK, scenariusze reagowania na ransomware i ataki DDoS czy demonstracje nowoczesnych rozwiązań klasy XDR.

Dla samorządów może to być także wartościowa propozycja dla pracowników działów IT oraz osób odpowiedzialnych za bezpieczeństwo systemów informatycznych w urzędach i jednostkach podległych, którzy podczas kongresu będą mogli poszerzyć wiedzę o aktualnych technikach ataków oraz metodach ich wykrywania i neutralizowania.

Integralną częścią wydarzenia będzie również strefa EXPO, w której firmy technologiczne zaprezentują rozwiązania wspierające bezpieczeństwo systemów informatycznych, ochronę danych oraz zarządzanie incydentami cybernetycznymi.

Organizatorzy podkreślają, że celem kongresu jest stworzenie przestrzeni wymiany wiedzy pomiędzy administracją publiczną, sektorem prywatnym i środowiskiem eksperckim. W obliczu rosnących zagrożeń w cyberprzestrzeni budowanie odporności cyfrowej instytucji publicznych – w tym samorządów – staje się jednym z kluczowych elementów bezpieczeństwa państwa.

Szczegółowy program, aktualną listę wystawców oraz informacje o rejestracji można znaleźć na stronie insecon.pl

Wydarzenie zostało objęte patronatem medialnym przez Dziennik Warto Wiedzieć.