



Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

10 listopada 2026 r.

Typ 200

Projektowanie bezpiecznej architektury sieci

Dynacon Sp. z o.o.

10.00 - 10.05

Zasady organizacyjne przebiegu szkolenia

Przedstawiciel Departamentu Cyberbezpieczeństwa MC

10.05 - 10.15

Architektura sieci jako fundament cyberbezpieczeństwa

- dlaczego bezpieczeństwo zaczyna się od architektury, a nie od wyboru urządzeń? Podstawowe zasady projektowania: segmentacja, separacja funkcji, strefy bezpieczeństwa, kontrola komunikacji i ograniczanie skutków kompromitacji.
- podstawowe zasady projektowania: segmentacja, separacja funkcji, strefy bezpieczeństwa, kontrola komunikacji i ograniczanie skutków kompromitacji.

Ekspert „Dynacon”: Barbara Szymańska

10.15 - 10.40

Case study 1 – Bezpieczeństwo brzegowe: jedno urządzenie, wiele funkcji, jeden punkt kompromitacji

- analiza architektury skupiającej routing, dostęp zdalny, ochronę brzegową i komunikację między segmentami na jednym urządzeniu
- konsekwencje kompromitacji, problemy z separacją funkcji i kontrolą komunikacji
- projektowanie bezpiecznych stref brzegowych, wydzielanie funkcji i wielowarstwowa ochrona

Ekspert „Dynacon”: Barbara Szymańska

10:40 - 11.00	Case study 2 – Bezpieczeństwo chmurowe: czy przeniesienie infrastruktury do chmury oznacza bezpieczeństwo? • błędy w projektowaniu połączeń między środowiskami lokalnymi a chmurą, niewłaściwa segmentacja zasobów, nadmierne uprawnienia i brak kontroli przepływów komunikacyjnych • projektowanie bezpiecznej architektury hybrydowej, separacja środowisk i kontrola dostępu <i>Ekspert „Dynacon”: Barbara Szymańska</i>
11.00 - 11:25	Case study 3 – Bezpieczeństwo wewnętrzne IT: jedna sieć, wiele VLAN-ów, pozorne bezpieczeństwo • dlaczego VLAN nie jest wystarczającym mechanizmem segmentacji bezpieczeństwa? • analiza sieci z centralnym routingiem i niekontrolowaną komunikacją między segmentami. • ruch lateralny, separacja systemów krytycznych, mikrosegmentacja i kontrola komunikacji wewnętrznej. <i>Ekspert „Dynacon”: Barbara Szymańska</i>
11.25 - 11.50	Case study 4 – Bezpieczeństwo wewnętrzne OT: kiedy sieć przemysłowa staje się przedłużeniem IT • analiza błędów w projektowaniu sieci przemysłowych: płaska architektura, brak separacji systemów technologicznych, bezpośrednia komunikacja IT–OT • niekontrolowany dostęp serwisowy • Projektowanie stref bezpieczeństwa i kanałów komunikacyjnych, segmentacja OT, ochrona systemów sterowania oraz bezpieczna integracja IT/OT <i>Ekspert „Dynacon”: Barbara Szymańska</i>
11.50 - 12.00	Od błędnej architektury do bezpiecznego projektu – najważniejsze zasady • podsumowanie wspólnych błędów projektowych • jak analizować architekturę pod kątem bezpieczeństwa? • jak identyfikować krytyczne zależności, punkty kompromitacji oraz niekontrolowane przepływy komunikacyjne? <i>Ekspert „Dynacon”: Barbara Szymańska</i>
12.00-12.10	Sesja pytań i odpowiedzi do ekspertów <i>Ekspert „Dynacon”: Barbara Szymańska</i>