SamorządIT

Argument dla przełożonego

Krótki materiał do przekazania sekretarzowi, kierownikowi jednostki albo osobie decydującej o budżecie: dlaczego wdrożenie podstaw cyberbezpieczeństwa w JST jest decyzją o ograniczeniu ryzyka, a nie zakupem „kolejnych dokumentów”.

Teza do rozmowy

Koszt uporządkowania dokumentacji, ról, rejestrów i reakcji na incydent jest niższy niż koszt jednego poważnego zdarzenia: ransomware, wycieku danych, przestoju systemów albo audytu, w którym jednostka nie potrafi pokazać dowodów działania.

SamorządIT traktuje dokumenty jako narzędzie wdrożenia. Celem jest to, żeby JST wiedziała: kto odpowiada, co sprawdzamy, co zapisujemy, komu eskalujemy i jaki dowód zostaje po wykonaniu działania.

Najprostsze uzasadnienie decyzji

Ryzyko	Co grozi jednostce	Co porządkuje SamorządIT
Ransomware lub awaria	Przestój usług, presja decyzji, koszt odtwarzania.	Role, eskalację, ciągłość działania i dowody decyzji.
Wyciek danych	Notyfikacje, obsługa naruszenia, ryzyko kar i utraty zaufania.	Zasady dostępu, nośniki, incydenty, dokumentowanie działań.
Audyt KRI/KSC/NIS2	Brak wykazania działań mimo realnej pracy IT.	Polityki, rejestry, przeglądy i ślad odpowiedzialności.

Co faktycznie kupuje JST

Gotowy system wdrożenia cyberbezpieczeństwa: 3 filary, 14 modułów i 131 dokumentów, rejestrów, procedur oraz formularzy. Moduły można wdrażać etapami, zaczynając od największego braku organizacyjnego.

Proponowana ścieżka 30-60-90 dni

30 dni	Ład dokumentacyjny: aktywa, konta, poczta, nośniki, podstawy KRI.
60 dni	Reakcja: incydenty, role, eskalacja, analiza po zdarzeniu, monitoring.
90 dni	Gotowość organizacyjna: ciągłość działania, dostawcy, zamówienia, szkolenia, SZBI.

Decyzja do podjęcia

Nie trzeba kupować wszystkiego naraz. Wystarczy wskazać pierwszy etap: najczęściej Filar I i moduł M05 Podstawy KRI, jeśli jednostka nie ma jeszcze stabilnego minimum dokumentacyjnego.

Strona systemu: www.samorzadit.pl/o-systemie · Katalog modułów: www.samorzadit.pl/moduly · Kontakt: kontakt@samorzadit.pl