

Wzmocnij cyberbezpieczeństwo w sektorze publicznym



Rozwiązania cyberbezpieczeństwa dla samorządów

1. Testy socjotechniczne + szkolenie budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST (szkolenie online z możliwością nagrania)

Jak dbać o bezpieczeństwo

Cyklicznie edukuj pracowników w zakresie wiedzy na temat cyberbezpieczeństwa. Wykorzystaj test socjotechniczny oparty na symulacji phishingu.

Dlaczego

Aby zwiększać czujność pracowników wobec zagrożeń i uczyć odpowiedniej reakcji na nie. Aby zwiększyć poziom bezpieczeństwa w JST.



2. Opracowanie dokumentacji SZBI + audyt SZBI



Jak dbać o bezpieczeństwo

Zleć zewnętrzny przegląd i ocenę procesów bezpieczeństwa informacji pod kątem ich zgodności z normą ISO 27001 lub innymi wytycznymi, np. KRI/KSC. Zwiększ świadomość występowania luk i wynikających z nich zagrożeń. Zapoznaj się z możliwymi kierunkami rozwoju poziomu dojrzałości bezpieczeństwa.

Dlaczego

Aby spełnić obowiązek prawny regularnego przeprowadzania przeglądów bezpieczeństwa informacji. Aby pozyskać wiedzę na temat odporności organizacji na cyberataki (poprzez przeprowadzenie przeglądu).

3. Bezpieczny internet (ZUTM/ONS/OIP)



Jak dbać o bezpieczeństwo

Zabezpiecz sieć przed cyberzagrożeniami. Monitoruj wykorzystanie internetu i określaj reguły dostępu do stron WWW. Stosuj ochronę przed atakami DDoS.

Dlaczego

Aby zapewnić nieprzerwane działanie usług internetowych oraz ochronę łącza.

4. Bezpieczny pracownik (AV/MDM/CyberWatch)



Jak dbać o bezpieczeństwo

Chroń komputery pracowników, infrastrukturę techniczną, urządzenia przenośne. Efektywnie zarządzaj flotą urządzeń mobilnych oraz komputerów przenośnych.

Blokuj podejrzane strony WWW na swoim łączu i na urządzeniach mobilnych.

Dlaczego

Aby chronić firmę przed malware'em, ransomware'em, phishingiem, kradzieżą i wyciekami danych firmowych. Aby zapewnić standaryzację sposobu używania firmowego sprzętu oraz aplikacji.

5. Bezpieczne dane (SOC Lite/DLP/CyberPakiet)



Jak dbać o bezpieczeństwo

Chroń ważne dane udostępniane w organizacji przed ich utratą i wyciekami. Monitoruj incydenty bezpieczeństwa. Monitoruj bezpieczeństwo swojej infrastruktury i web aplikacji. Kontroluj reputację swoich domen.

Dlaczego

W celu wykrywania prób kradzieży wrażliwych danych mieszkańców i/lub pracowników samorządu.

Oferta

Umożliwiamy zakup produktów i usług w modelu jednorazowym i abonamentowym. Program Partnerski – pracujemy z zaufanymi partnerami IT wskazanymi przez Orange lub klienta.