ZARZĄDZANIE PARAFIĄ

Bezpieczeństwo parafii i duchownych

w sieci

FabrykaWiedzy

PROFESJONALNE WSPARCIE
W CODZIENNEJ PRACY

ODKRYJ WIĘCEJ PUBLIKACJI I SKORZYSTAJ Z RABATÓW

Zeskanuj kod lub wejdź na stronę
https://ln.wip.pl/fabrykawiedzy

Bezpieczeństwo parafii i duchownych w sieci

Copyright © Warszawa 2026 by Wiedza i Praktyka sp. z o.o

Autor: Jakub Kwaśnik, Marcin Sarna
Redakcja: Anna Konarzewska-Żuczek
Korekta: Zespół
Koordynator produkcji: Mariusz Jezierski
Koordynator projektów wydawniczych: Anna Jagodzińska
Content & Publishing Leader: Marta Grabowska-Peda

Projekt graficzny okładki: Agnieszka Makowska
Zdjęcie na okładce: Freepick
Skład i łamanie: Agnieszka Makowska

Wydanie I
Stan prawny: kwiecień 2026 r.
ISBN: 978-83-8409-639-0
Kod produktu: 1QS010

Wydawca:
Wiedza i Praktyka sp. z o.o.
03-918 Warszawa, ul. Łotewska 9a
tel. 22 518 29 29, faks 22 617 60 10
www.wip.pl

Publikacja uwzględnia stan prawny obowiązujący na dzień 1 kwietnia 2026 r.

Niniejsza publikacja oraz wszystkie zawarte w niej teksty, grafiki i materiały są chronione prawem autorskim. Żadna część tego e-booka nie może być reprodukowana, przechowywana w systemach wyszukiwania lub transmitowana w jakiejkolwiek formie i jakimikolwiek środkami – elektronicznymi, mechanicznymi, kopiowania, nagrywania lub innymi – bez uprzedniej pisemnej zgody Redakcji.
Zakaz ten nie dotyczy cytowania ww. materiałów w granicach dozwolonego użytku, z powołaniem się na źródło.

Treści zawarte w niniejszej publikacji mają charakter wyłącznie informacyjny i edukacyjny. Publikacja została przygotowana z zachowaniem najwyższej staranności oraz z wykorzystaniem wysokich kwalifikacji, wiedzy i doświadczenia autorów oraz konsultantów. Niemniej jednak zawiera ona ogólne wskazówki i nie powinna być traktowana jako indywidualna porada prawna, finansowa, medyczna ani żadna inna forma profesjonalnej konsultacji.

Redakcja nie ponosi odpowiedzialności za decyzje podjęte na podstawie informacji zawartych w tej publikacji. W przypadku potrzeby uzyskania specjalistycznej porady zaleca się konsultację z odpowiednim ekspertem lub specjalistą w danej dziedzinie.

Spis treści

Zabezpieczenia w parafii związane z cyberprzestępczością 5

Kradzież tożsamości w Internecie 11

Hejt - cyfrowy sztylet 18

Na jakie rodzaje cyberataków narażona jest parafia? 24

Pułapki prawne przy kupnie programów komputerowych dla parafii 33

Ochrona danych osobowych w zasobach informatycznych parafii 43

Zabezpieczenia w parafii związane z cyberprzestępczością

Statystyki związane z cyberprzestępczością są nieubłagane: z roku na rok rośnie liczba zagrożeń w sieci, a metody sprawców stają się coraz bardziej wyrafinowane i skuteczne. Jak zatem możemy zadbać o bezpieczeństwo powierzonych nam danych i informacji? Nasze działania powinny skupić się na dwóch podstawowych obszarach. Pierwszym z nich jest podnoszenie własnej świadomości na temat zagrożeń w sieci, gdyż wykształca ona pewną ostrożność i czujność na niepokojące zjawiska. Drugim obszarem działań, jakie możemy podjąć, jest inwestycja w odpowiednie zabezpieczenia, które – co ważne – mają sens jedynie wówczas, gdy towarzyszą świadomości i ostrożności jako czynności wspierające.

Gdy podnosimy własną świadomość istniejących zagrożeń, jeśli poznamy najpopularniejsze metody działań cyberprzestępców opartych na socjotechnice, łatwiej nam będzie zdroworozsądkowo ocenić, czy nietypowa sytuacja bądź prośba może być próbą wyłudzenia danych. Jeśli odpowiednio wcześnie rozpoznamy przesłanki, które obudzą naszą czujność, będziemy mogli zweryfikować działania sprawcy, poprosić o uwiarygodnienie danej prośby i to pozwoli nam skutecznie zablokować atak i ochronić dane.

Stosując zaś różne zabezpieczenia, należy pamiętać, że nawet kosztowne nie będą dla nas żadną gwarancją bezpieczeństwa, jeśli będziemy popełniać szkolne błędy (jak w przypadku podręcznikowego przy kładu, w którym firma wydała setki tysięcy złotych na zabezpieczenia sieci i urządzeń, a jeden z członków zarządu o szerokich uprawnieniach w systemie pozostawił w biurze laptopa z przypiętą do ekranu karteczką z hasłem dostępowym). Stąd też chciałbym zaprezentować działania, które pozwolą w parafii/instytucji kościelnej na lepszą i skuteczniejszą ochronę powierzonych danych.

Po pierwsze, warto inwestować w szkolenia oraz audyty, które pozwolą poszerzyć świadomość zagrożeń i zdiagnozować istniejące ryzyko, dotyczy to również parafii. Znaczna część organizacji rozpoczyna pracę nad bezpieczeństwem informacji od zasięgnięcia informacji u specjalisty, który przyjrzy się indywidualnym potrzebom i opracuje odpowiedni plan bądź dobierze zabezpieczenia dla konkretnego podmiotu. Pozostałe instytucje traktują szkolenia jako dopełnienie własnych wypracowanych zabezpieczeń.

WAŻNE

Nawet jednorazowa konsultacja potrafi być bardzo pomocna dla wszystkich tych jednostek i osób, które dotychczas nie miały okazji zetknąć się z wyzwaniami dotyczącymi ochrony danych.

Nie istnieją uniwersalne metody działania w tym obszarze, każda parafia bowiem, podobnie jak każdy podmiot komercyjny, posiada własną specyfikę funkcjonowania (zasoby, charakter realizowanych projektów, wielkość baz danych), jak też własną specyfikę zagrożeń (ekspozycję na określone typy przestępczości bądź czynniki ryzyka). W przypadku parafii jedną z osób, które możemy poprosić o konsultację, jest na przykład Diecezjalny Inspektor Ochrony Danych.

Dokumentacja – każda parafia, instytucja oraz jednostka kościelna posiada bogatą dokumentację zarówno w wersji papierowej, jak i elektronicznej, która powinna być odpowiednio zinwentaryzowana i opisana. Jeśli będziemy posiadać rzetelny rejestr zbiorów, którymi dysponujemy, pozwoli nam to odpowiednio zorganizować codzienną pracę i stworzyć skuteczny mechanizm ochrony informacji. Systematyka powinna zawierać informacje na temat określonego obszaru dokumentów, np. ekonomiczne, archiwalne, związane z obowiązkami kanonicznymi, zawierające dane osobowe oraz formy przechowywania (papierowa, elektroniczna). Niekiedy przepisy szczegółowe lub zalecenia organów nadrzędnych zawierają dodatkowe wskazania co do zakresu dokumentacji, np. przepisy związane z ochroną danych informują o potrzebie posiadania rejestru osób upoważnionych do przetwarzania danych lub o dobrej praktyce istnienia rejestru incydentów. Bardzo ważne jest odpowiednie przechowywanie dokumentacji. Kancelaria parafialna powinna posiadać odpowiednie zabezpieczenia przed nieuprawnionym dostępem osób trzecich do dokumentów. Pomieszczenie powinno posiadać fizyczne zabezpieczenia, jak np. kraty w oknach lub żaluzje antywłamaniowe, powinno być również zamykane na klucz, który będzie przechowywany w sposób pozwalający na zachowanie bezpieczeństwa. Monitor komputerowy w kancelarii nie powinien być zwrócony w stronę okna. W kancelarii powinna znajdować się zamykana, przeciwpożarowa szafa na najważniejsze dokumenty, a jeśli jest to możliwe – również sejf i niszczarka o odpowiednim poziomie rozdrabniania dokumentów. Musimy zdawać sobie sprawę, że także w tych dokumentach, które uznajemy za niepotrzebne lub zdezaktualizowane, może znaleźć się wiedza, która będzie cenna dla cyberprzestępcy. Jakiekolwiek informacje o sposobach wewnętrznej organizacji, pracownikach czy charakterze przetwarzanych danych mogą zostać wykorzystane do planowania kolejnych faz ataku. Jeśli przetwarzamy istotne zbiory w wersji elektronicznej, powinniśmy zadbać o sporządzanie regularnych kopii zapasowych na zewnętrznych nośnikach. Do kancelarii powinien być ograniczony dostęp osób nieuprawnionych, nie można również pozostawiać

obcych osób samych w takim pomieszczeniu. Komputery powinny być wyposażone w legalne, aktualne oprogramowanie, aplikację antywirusową oraz silne hasła dostępowe.

Polityka hasłowa – w przypadku dokumentacji przetwarzanej w formie elektronicznej, a także przy dokonywaniu operacji na bazach danych lub podczas korzystania z usług internetowych, często jedynym zabezpieczeniem jest kombinacja loginu i hasła. W tych serwisach, gdzie jest to możliwe, zachęcam do korzystania z tzw. dwuskładnikowego uwierzytelniania (2-FA), co oznacza, że dla wykonania danej operacji powinniśmy np. wprowadzić dodatkowy kod przesyłany drogą SMS-ową lub skorzystać z tokena (urządzenie generujące jednorazowe kody uwierzytelniające operację). Na rynku istnieją tak zwane klucze sprzętowe U2F (małe urządzenie podłączone do portu USB, którego obecność jest wymagana do uruchomienia określonego programu), które pozwalają odpowiednio zabezpieczyć proces logowania. Niezależnie, czy zdecydujemy się na korzystanie z powyższych rozwiązań, sprawą konieczną jest zadbanie o bezpieczne hasło. Jednym z najczęstszych i najbardziej podstawowych błędów jest tworzenie prostych, łatwych do skojarzenia i zapamiętania haseł opartych na rutynowych, intuicyjnych skrótach myślowych.

PRZYKŁAD:
Na potrzeby niniejszego tekstu załóżmy istnienie Parafii pw. św. Jakuba w Rogalicach przy ulicy Klasztornej 5, gdzie Księdzem Proboszczem jest ks. Piotr Iksiński, urodzony 24.07.1964 r. Na podstawie analizy popularności określonych schematów myślowych wykorzystywanych przez typowych użytkowników można wskazać przykładową grupę haseł, które charakteryzują się wysokim prawdopodobieństwem użycia: Jakub5, swJakub5, Klasztorna5, Klasztorna123, Giacomo24, StJames64, Piotr1!, Piotr1964, Piotr2407, Jakub2407, Jakub1964, Klasztor na1964, Rogalice1964, IksinskiP1964, Piotrek5, 24071964, PiotrX.