Twee op de drie websites Friese kerken onveilig

Ethische hack legt zorgelijke situatie kerkgemeenten bloot

Jan-Peter Soenveld

Leeuwarden | Veel kerkgemeenten in Fryslân hebben hun websites niet goed beveiligd. Daardoor kunnen kwaadwillenden websites aanpassen of dreigt zelfs gegevensdiefstal. Dat blijkt uit een steekproef van Hacklab, uitgevoerd in opdracht van het *Friesch Dagblad*. Het onderzoek geeft een sterke indicatie voor de digitale situatie in heel kerkelijk Nederland.

Hacklab in Leeuwarden, onderdeel van MKB Cybercampus, leidt jongeren op tot ethische hackers. Dat zijn computerspecialisten die inbreken in systemen om ze te controleren op veiligheid. Met die bevindingen worden eigenaren geholpen hun beveiliging op orde te brengen.

De hackers bekeken in deze steekproef de afgelopen tijd 29 websites van Friese kerkgemeenten, verspreid over de provincie, en van verschillende gezindte en grootte. Ze voerden een voorzichtige penetratietest (pentest) uit, waarbij de hackers niet in de systemen zelf kwamen. ,,We kijken of de deur van het slot gehaald kan worden, maar gaan niet naar binnen", zegt hacker Wino Bouwens.

Bij twee derde van de kerkelijke webpagina's waren er enige tot forse beveiligingsrisico's. Bij drie sites werden ernstige tekortkomingen gevonden. ,,Eentje konden we met een paar drukken op de knop platleggen", aldus Bouwens. Bij een andere gemeente hadden de hackers kunnen binnendringen om zaken te veranderen. ,,Bijvoorbeeld een virus installeren."

Bij zeven websites werden kwetsbaarheden gevonden waardoor hackers wachtwoorden kunnen achterhalen, of de website kunnen inzetten bij een ddos-aanval. Bij zo'n ddos-aanval wordt een website platgelegd door vanuit andere systemen (zoals een kerkwebsite) grote hoeveelheden data te sturen. De afgelopen weken werden bijvoorbeeld bij csg Comenius Mariënburg in Leeuwarden en internetprovider KabelNoord uit Dokkum slachtoffer van zo'n aanval.

Bij nog eens tien websites wisten de hackers gebruikersnamen te achterhalen. Met die informatie proberen datadieven vaak wachtwoorden te ontfutselen. Bij elf websites stonden tien of meer digitale poorten open. Dit is niet per se onveilig, maar wel een onnodig risico.

Ook vonden hackers verouderde software. ,,Als de software niet up-to-date gehouden wordt, kunnen er in de toekomst kwetsbaarheden ontstaan", zegt hacker Melle Popma. Het viel verder op dat de websites met de minste digitale functies, zoals antwoordformulieren, ook de minste kwetsbaarheden vertoonden.

Ook andere organisaties

Erik Rutkens, voorzitter van de Stichting Cyber Security Centrum Noord-Nederland, vermoedt dat ook bij andere maatschappelijke organisaties, zoals sportverenigingen, de digitale veiligheid te wensen overlaat. Veel van die organisaties hebben op hun website persoonsgegevens staan. ,,En die kunnen veel geld waard zijn voor cybercriminelen."

Met die gegevens (e-mailadressen en wachtwoorden) kunnen criminelen ook inbreken in systemen. ,,Als je bent ingelogd met je hotmailaccount, is de kans groot dat je die gegevens ook gebruikt voor Facebook. En criminelen kunnen met persoonsgegevens identiteitsfraude plegen."

Rutkens ziet voor kerken een extra risico in de digitale onveiligheid. ,,Er is sprake van polarisatie in de samenleving, ook wat betreft antireligieuze gevoelens. En als een voorganger in IJlst iets zegt waar een moslim of atheïst in Zeeland niet blij mee is, moest die laatste vroeger vier uur rijden om de ramen van de kerk in te gooien. Nu kan hij in een paar seconden de website hacken." De kerkgemeenten zijn op de hoogte gesteld van de kwetsbaarheden. De hacktest is in overleg met de politie gedaan.