Hoe veilig is de website van de kerk eigenlijk?

Het is soms ergerlijk eenvoudig om in te breken in een website van een kerkgemeente. Twee hackers van het Hacklab in Leeuwarden bekeken in opdracht van het *Friesch Dagblad* 29 websites van Friese kerkgemeentes om te kijken of de getroffen veiligheidsmaatregelen voldoende waren. Bij eentje namen ze de krant mee in dat proces. Dat onveiligheid grote gevolgen kan hebben, ondervond een kerk in Burgum eerder. Het is gelukkig niet moeilijk om de risico's te beperken, vertelt cyberspecialist Erik Rutkens.

Jan-Peter Soenveld Marchje Andringa

Ik ga even naar deze *source-code* kijken. Elke browser heeft *developmenttools*. Als je die opent, krijg je dit schermpje. Hier kan weeens informatie in staan, die je kan *exploiten*. Bijvoorbeeld als de software van Wordpress niet up-to-date is." Het vakjargon vliegt om de oren, wanneer hackers Melle Popma (28) en Wino Bouwens (26) van het Hacklab in Leeuwarden een website van een Friese kerkgemeente proberen te kraken.

Popma en Bouwers zijn zogeheten ethische hackers. Ze zoeken kwetsbaarheden op en melden dat aan de eigenaar van het systeem, bijvoorbeeld een website. Zo wordt voorkomen dat een kwaadwillende hacker de website kraakt.

Al vrij snel nadat ze zijn begonnen en de eerste scans hebben uitgevoerd, wordt duidelijk dat de kerkwebsite op een verouderde versie van Wordpress draait. Dit is een programma om websites te maken. „Hoe meer ze achterlopen, hoe meer kwetsbaarheden er zijn", vertelt Bouwens. De Wordpress-versie is een half jaar oud, terwijl het volgens de hackers vrij eenvoudig is om die up-to-date te houden.

Verzoek

Hackers kunnen talloze programma's (*tools*) gebruiken om digitaal in te breken. Bouwens pakt er eentje bij, genaamd Burpsuite. „Elke keer als je als gebruiker naar een website gaat, stuur je een *request* (verzoek) of je de website mag zien", legt hij uit. „Dat is hoe het standaard gaat. Maar met deze tool manipuleren we het verzoek."

Zo kan Bouwens bijvoorbeeld een code naar de website sturen om te kijken of die een opdracht uitvoert. „Stel, we geven de website de opdracht: *say hello* (zeg hallo), dan kan de website ons 'Hello' sturen." En inderdaad, de website doet wat Bouwens opdraagt. „Dat is heel onhandig", legt hij uit. „Want ik kan de website dan ook een verzoek laten sturen naar een ander systeem. De website kan zo een onderdeel worden in een ddos-aanval." Bij zo'n aanval worden zo veel verzoekjes verstuurd naar een derde website, dat die al die verzoeken niet kan verwerken en plat gaat.

Ook vindt Bouwens op vergelijkbare wijze een mogelijke manier om inloggegevens van kerkleden of beheerders opgestuurd te krijgen. „Wordpress geeft je de keuze om dit aan of uit te zetten." Geadviseerd wordt om dit uit te schakelen, omdat een website er kwetsbaar uitziet als een hacker zo'n slordigheid detecteert. Het is net als bij een huis: een inbreker kiest altijd voor het huis met de slechtste sloten.

Dit blijkt later de grootste dreiging te zijn op deze website, voor zover de hackers kunnen nagaan. In overleg met een jurist bij de politie morrelen ze wel aan het slot, maar gaan ze niet naar binnen.

Opeens onbereikbaar

Maar er zijn genoeg hackers die niet bij de voordeur stoppen. De Protestantse Gemeente Burgum werd vorig jaar slachtoffer van een hack. „Onze website was opeens niet meer bereikbaar", vertelt Romke van Groning, ICT'er van beroep en als vrijwilliger betrokken bij de kerk. Van Groning was ten tijde van de hack websitebeheerder.

De kerk had de website zelf gemaakt via het programma Joomla, en betaalde de internetprovider voor een back-upvoorziening, om de website te herstellen bij problemen. „We waren al twee keer eerder gehackt. Toen heeft de provider die hersteld met de back-up."

Ook bij de laatste hack werd de provider om hulp gevraagd. „Maar toen konden ze het niet herstellen. De provider was net gefuseerd en dat gaf allerlei problemen. Het werd een kastje-muurverhaal."

> Het is net als bij een huis: een inbreker kiest altijd voor het huis met de slechtste sloten

De kerk had het voordeel dat er uit voorzorg al weinig gevoelige informatie op de website stond. Niettemin was de kraak vervelend. „De website was een soort nieuwsvoorziening voor mensen die niet wekelijks naar de kerk konden. We hebben toen een tijdelijke website gemaakt, maar het duurde wel een tijdje voordat we een echte nieuwe website hadden." Ook konden de hackers enkele e-mailadressen van leden achterhalen.

Bij de nieuwe website heeft de kerk het zekere voor het onzekere genomen en is een professioneel bedrijf ingeschakeld. „Deze website is veiliger en gebruiksvriendelijker. De vorige website vergde veel onderhoud en het is lastig om vrijwilligers met technische kennis te vinden. Dat geldt, denk ik, voor veel kerken." Het ICT-bedrijf zorgt er onder meer voor dat de website tijdig veiligheidsupdates krijgt en is bereikbaar bij calamiteiten.

Van Groning adviseert andere kerken hetzelfde te doen. „De gemiddelde kerk heeft de kennis niet in huis. Iedereen kan wel een website in elkaar flansen, maar als je iets goed wilt doen heb je een stukje professionaliteit nodig."

Brute force attack

De website die de ethische hackers onder handen nemen, lijkt weinig professioneel. Zo weet Popma al snel via een andere scan twee gebruikersnamen te achterhalen. Een hacker kan vervolgens een 'brute force attack' uitvoeren om ook het wachtwoord te achterhalen. Bij zo'n aanval worden miljoenen wachtwoorden geprobeerd, met een snelheid van duizenden per seconde. „En je hebt bijvoorbeeld lijsten met de duizend meest gebruikte wachtwoorden van Nederland", vertelt Popma „Hoe groot dit risico is, hangt af van het wachtwoord. Als de gevonden gebruikers een zwak wachtwoord hebben, is het een kwestie van tijd voordat een hacker dat raadt."

Ook bij een scan op de digitale poorten van de website stuiten de hackers op een mogelijk risico. „Je kunt via het internet naar een IP-adres", legt Popma uit. Een IP-adres is een digitaal postadres. „Daar kan je pakketjes naar versturen. Dat gaat via poorten. Alle software die je op een website gebruikt, heeft een poort."

Er zijn in totaal zo'n 65.000 poorten en de hackers hebben een eenvoudig programma waarmee ze de duizend meest gebruikte wachtwoorden in een paar minuten kunnen controleren. Hoe meer poorten dicht staan, hoe beter. Wino laat als voorbeeld een poortscan zien van www.nu.nl, waar twee poorten open staan (HTTP en HTTPS). „Dat zijn poorten waarmee bezoekers op de website komen."

Bij de kerkelijke website staan 22 poorten open. Dat is niet per se gevaarlijk. „Niet elke open poort is een kwetsbaarheid. Maar als je bijvoorbeeld verouderde software hebt, is zo'n poort dat wel." In de tussentijd, na ongeveer anderhalf uur scannen, meldt Bouwens dat hij van de website is gegooid. „Dat is een goed teken", zegt hij. „De website heeft gemerkt dat ik iets doe dat niet koosjer is, en nu is mijn IP-adres geblokkeerd." Popma: „Maar het duurde wel even. Dus die blokkade kan misschien omzeild worden."

Bij een paar andere scans worden geen evidente kwetsbaarheden gevonden. Zo checken ze of ze kunnen zien welke bestanden op de website zijn gezet. „Maar dat is goed dichtgezet." Bouwens: „Bij een andere test vonden we een keer foto's van alle werknemers, met naam en achternaam." Ook lukt het niet om de website in te war te brengen door programmeertaal bij de zoekfunctie in te voeren.

Lek als een mandje

Naast deze website, werden nog 28 digitale Friese kerkensites gecontroleerd. Het veiligheidsbeeld wisselt. Sommige website zijn zo lek als een mandje, terwijl andere geen kwetsbaarheden toonden. Tot die laatste groep behoren vooral de websites met weinig functies.

Volgens Erik Rutkens, voorzitter van de Stichting Cyber Security Centrum Noord-Nederland, zijn veel van de kwetsbaarheden goed te voorkomen, als de digitale basiskennis op een hoger niveau komt. „Er zijn een paar kleine dingen die de wereld er al veel veiliger uit laten zien", denkt hij. „Bijvoorbeeld door regelmatig updates te installeren en sterke wachtwoorden te verzinnen."

Tegelijkertijd ziet hij dat veel van mensen gevraagd wordt bij het bestieren van een website. „Als je bijvoorbeeld een website met ledenadministratie wilt, heb je verschrikkelijk veel aanbieders. Je zou verwachten dat die dat goed voor elkaar hebben, maar in de praktijk is dat vaak niet het geval. Dus hoe weet je als kerkbestuurder nu dat je zaken doet met iemand die veilig werkt?"

> Het is lastig om vrijwilligers met technische kennis te vinden. Dat geldt, denk ik, voor veel kerken

Veel van de gevonden kwetsbaarheden vallen volgens Rutkens onder de verantwoordelijkheid van de websiteleveranciers. Zoals het sluiten van de digitale poorten. „22 poorten open is gewoon heel veel", zegt hij over de website die de hackers samen met het *Friesch Dagblad* bekeken. „Daar moet de leverancier iets aan doen, vind ik."

Bij veel van de websites die de hackers bekeken was de software niet up-to-date, ook een verantwoordelijkheid van de leverancier. „En dat is vragen om ellende. Er zijn scans die het automatisch internet afstruinen en die kunnen zo'n kwetsbare website vinden. In het ergste geval kan iemand dan *ransomware* (gijzelsoftware) installeren of de inhoud van de website veranderen."

Hij vindt het verder opmerkelijk dat de hackers bij de websites veel gebruikersnamen vonden. „Er zijn op het darkweb (het deel van het internet waar je niet met standaard browsers op kunt komen, JPS) databases met mailadressen en wachtwoorden, op basis van eerdere lekken. Als een gebruikersnaam daarin staat, kunnen de hackers kijken of ze dit wachtwoord ook bij de kerkwebsite kunnen gebruiken."

En vaak is zo'n database niet eens nodig, omdat mensen simpele wachtwoorden als 'welkom' of 'admin' gebruiken. Hackers kunnen de gebruikersnamen ook gebruiken om in te loggen op andere systemen. „Zoals Webkamp. En dan kunnen ze een bestelling doen en elders laten bezorgen. Dat soort dingen wil je gewoon niet."

Het is daarom vooral zaak om de basiszaken goed voor elkaar te hebben. „Op het moment dat jij al iets aan beveiliging hebt gedaan, kost het hackers moeite om binnen te komen. Als dat bij bijvoorbeeld de gereformeerde kerk wel is gedaan en bij de katholieke kerk niet, dan zullen hackers altijd voor de katholieke kerk kiezen."

De digitale risico's voor kerken zullen de komende jaren alleen maar toenemen, vreest hij. „Als je kijkt naar hoe de digitale gemeenschap zich ontwikkelt, dat zie je dat daar een gigantische polarisatie plaatsvindt. En je merkt het ook aan online criminaliteit. Criminelen wanen zich online veiliger dan in de fysieke wereld. Als ik wil inbreken, dan horen mensen het als ik een steen door een raam gooi", zegt Rutkens. „Zo ervaren mensen een drempel. Online is die drempel er minder. Op het moment dat iemand van een kerkgemeenschap zijn mening ergens zou uiten, dan kan het zijn dat iemand die daarop tegen is naar digitale middelen grijpt om zijn gelijk te krijgen. Dus ik denk dat het risico steeds groter wordt, helaas."