Hoe beveilig je je website?

Joep Bär

En hoe houd je deze beschermd?

Open-source Content Management Systemen (CMS'en) zoals WordPress, Drupal en Joomla, zorgen ervoor dat websites vanaf de start een groot aantal functies beschikbaar hebben die helpen om een veelheid van soorten pagina's (incl. formulieren) te kunnen gebruiken en het aantal bezoekers te verhogen. Miljoenen websites draaien op een CMS, maar webbeheerders maken zich nog steeds terecht zorgen over de veiligheid van hun websites. Veel websites vragen bezoekers om verschillende redenen om hun persoonlijke gegevens. Ze slaan ook hun login-informatie op, terwijl e-commerce sites ook de financiële informatie van de bezoekers opslaan. Daarom is het noodzakelijk ervoor te zorgen dat het platform (webhosting en website) veilig is om een datalek te voorkomen.

Up-to-date houden van de site

Net als alle andere applicaties moet een website altijd worden bijgewerkt naar de nieuwste versies. Deze bevatten nieuwe beveiligingsfuncties en/of functionaliteit van het CMS zelf of van reeds geïnstalleerde plug-ins/modules. Maak alleen gebruik van vertrouwde plug-ins/modules en thema's om een veilige website te garanderen.
De beheerder kan via admin portal gemakkelijk controleren of er updates beschikbaar zijn. In ieder geval kan bij WordPress en Drupal gebruik worden gemaakt van een automatische signalering van updates. Ieder CMS heeft zijn eigen methode voor het installeren van de nieuwste versies. Maak altijd vóór een update een betrouwbare back-up van de website.

Maak back-ups

Er kan zich een onvoorziene gebeurtenis voordoen die schade kan toebrengen aan de website. Hoewel dergelijke gebeurtenissen niet te voorspellen zijn, moeten webbeheerders erop voorbereid zijn. De schade kan worden beperkt door regelmatig een back-up van de website te maken. Het maken van een back-up moet hoog op de veiligheidschecklist staan.
Het is natuurlijk mogelijk een back-up op de webserver te maken, maar kwaadwilligen proberen deze te vinden om deze te downloaden en er misbruik van te maken. Zorg dus dat deze op een voor bezoekers onbereikbare plaats op de server staat. Beter is het om back-ups naar een andere server of een NAS te sturen.

Gebruik originele gebruikersnamen

Op ieder CMS moet ingelogd kunnen worden. Ofwel alleen door één beheerder, ofwel door alle personen van een groep (een familie, vereniging of organisatie). Zorg er in ieder geval voor dat de standaard gebruikersnaam van de beheerder NIET wordt gebruikt. Vaak is dit admin of administrator. Wijzig dit in iets als 'ikbenDeadmin' of een andere creatieve naam. Ook de andere personen met een inlogaccount moeten bij voorkeur een niet direct naar de persoon herleidbare naam krijgen. Zorg ervoor dat de inlog-/gebruikersnamen niet zichtbaar zijn als auteur van een artikel of op andere plaatsen. Dan is alleen nog het raden van het wachtwoord nodig om in te kunnen loggen.

Volg een sterk wachtwoordbeleid

Sterke wachtwoorden zijn de essentie van websitebeveiliging. Je moet een robuust wachtwoordbeleid hebben dat ervoor zorgt dat de gebruikers sterke wachtwoorden gebruiken voor hun toegang tot de website. Iedereen moet sterke wachtwoorden gebruiken, dus zowel de webbeheerders als de andere gebruikers. Volg voor sterke wachtwoorden de wereldwijde best practices. Zorg er altijd voor dat de wachtwoorden sterk zijn door complexiteit en dat ze tekens en alfabetten combineren, maar niet noodzakelijk in een volgorde. Vaak hebben CMS'en een of meer plug-ins of modules die sterke wachtwoorden afdwingen.
Ook op internet zijn voldoende websites die hierbij kunnen helpen.

Dubbele authenticatie instellen

Een sterkere vorm van wachtwoordcontrole is dubbele authenticatie ofwel Two-Factor Authentication (2FA). Het authenticatiemechanisme met twee factoren vereist het bezit van een fysiek apparaat. Als extra veiligheidsvoorziening moet de gebruiker een code invoeren om in te loggen. De code wordt naar het door de gebruiker geselecteerde apparaat gestuurd. Lees hierover meer in de artikelen van Rein de Jong in de laatste SoftwareBussen.

Inlogveiligheid

Zorg ervoor dat het aantal inlogpogingen beperkt is. Meestal zal dit gebaseerd zijn op een maximum aantal per IP-adres (een wereldwijd uniek adres per aansluiting op het internet) binnen een bepaalde tijd. Daarenboven zouden ook specifieke IP-adressen geheel geblokkeerd kunnen worden.
Controleer regelmatig of er overschrijdingen van de inlogliniet zijn geweest of laat de programmatuur automatisch een e-mail sturen naar de beheerder. Als blijkt dat een wachtwoord geraden is van een account, zorg dan dat dit zo snel mogelijk wordt aangepast en kijk of er schade is aangebracht. In voorkomende gevallen moet hiervan volgens de AVG-richtlijn melding worden gemaakt.

Beperk de toegang tot gebruikersaccounts

Een van de ideale security best practices is het beperken van de toegang via inlogaccounts. De gebruikers die toegang

hebben tot het beheergedeelte (de back-end) dragen bij aan het veiligheidsrisico van de website. De webbeheerders moeten de toegang beperken tot alleen degenen die toegang nodig hebben, en dat ook voor een bepaalde tijd. De beheerders moeten regelmatig de gebruikersaccounts controleren en zich bewust blijven van wie allemaal (volledige) toegang tot de back-end hebben en of ze de toegang nog steeds nodig hebben.
Stel het CMS zo in dat de diverse gebruikers (waaronder bezoekers) alleen toegang hebben tot het (beheer-)deel van de website die ze nodig hebben of mogen inzien. Geef, waar mogelijk, 'alleen-lezen'-toegang (dus zonder de mogelijkheid om inhoud te wijzigen) of de mogelijkheid om wel inhoud toe te voegen zonder inhoud te mogen wijzigen.

Spambescherming

Om een veilige website te garanderen, moet deze beschermd worden tegen spam. Installeer anti-spamfuncties, zoals plug-ins/modules die voorkomen dat spambots formulieren op de site kunnen invullen. Dat is effectief tegen verschillende spambots en is geschikt voor alle soorten formulieren op de site.
Het gebruik van een captcha, (rekensommetjes, plaatjes met een over te typen tekst of keuze van een aantal plaatjes) om te bewijzen dat je een persoon bent, is al lang de ideale manier om bots te blokkeren, maar niet de meest bezoekersvriendelijke. Captchas voorkomen het indienen van spam door bots en kunnen worden gebruikt voor elk webformulier dat op de gebruiker is gericht. Daarnaast zijn er vaak andere oplossingen om spam te filteren, bijvoorbeeld met de Akismet antispam diensten.

Zorg dat de basiscode van de website veilig is

De core (basiscode) moet altijd worden bijgewerkt naar de nieuwste versie. Als er zelf geschreven code wordt gebruikt mag hiervoor nooit de basiscode worden aangepast!
Als aanwezig, installeer dan een plug-in of module die controleert en meldt als de core aangepast wordt.

Databasebeveiliging

Als veiligheidsmaatregel moet de toegang tot de kritieke bestanden aan de back-end worden geblokkeerd. Zo kan de tabelprefix worden gewijzigd om het voor een indringer moeilijk te maken deze te raden en SQL-injecties te starten (code die achter een webadres geplaatst wordt om de databaseprogrammatuur te misleiden om gegevens uit de database te tonen). De tabel prefix kan, in ieder geval bij WordPress en Drupal, gewijzigd worden tijdens de installatie van een nieuwe website. Het is ook mogelijk om delen van de database versleutelen en eventueel de hele database.

Beveiliging van de webserver

De beheerder van de webhosting en van de website moeten de toegang tot de webserver beperken en tegelijkertijd de toegang tot de webserver voortdurend controleren. De serverhandtekening moet ook verborgen zijn, en houdt de poort nummers verborgen voor publieke toegang. Ook moet alle programmatuur van de webserver altijd worden bijgewerkt naar de laatste versie.
Zorg er daarom voor je website alleen bij een betrouwbaar webhostingbedrijf onder te brengen.

Installeer een SSL-certificaat

Het is essentieel om een SSL certificaat te installeren teneinde de website te beschermen. Door over te schakelen op

het HTTPS-protocol wordt de communicatie-uitwisseling met de browser van de bezoeker versleuteld. Zo kan geen derde partij kan toegang krijgen tot deze informatie, en de bron

wordt ook geauthentiseerd. Het kan man-in-the-middle-aanvallen (iemand die het verkeer tussen jouw browser en de webserver onderschept[1]) voorkomen en ervoor zorgen dat jouw website veiliger is. Bovendien kan het ook helpen bij SEO (Search engine optimization = betere vindbaarheid via zoekmachines) en de prestaties van de site verbeteren.

Wat beoogt een hacker?

Dat is uiteraard heel verschillend en afhankelijk van het doel van de hacker. Ze bestaan onder andere uit:
- Iets onschuldigs als het vervangen van de startpagina of alle pagina's met een banner van de hacker; (opmerking: plaatje hacked)
- Het volledig onbruikbaar maken van de website door gegevens te vernietigen. Heb je wel een back-up?
- Het stelen van gegevens, zoals e-mailadressen, creditcardgegevens en andere persoonlijke gegevens om deze te kunnen verkopen (vaak niet goed vast te stellen dat dit is gebeurd);

Het installeren van een programma om zo spamberichten te kunnen verzenden (vaak miljoenen in enkele dagen). Gevolg: de webserver komt op zwarte lijsten te staan en het kan weken duren voordat het mailverkeer van iedere website op die server weer normaal functioneert.

Hoe bereikt een hacker de website?

Natuurlijk heb je hackers die gewoon achter hun pc zitten en proberen in te loggen of via bekende zwakke plekken van het CMS toegang willen krijgen. Dit is natuurlijk erg arbeidsintensief en loont alleen als van de doelwebsite bekend is dat deze iets interessants te bieden heeft.
Daarom proberen hackers via zogenaamde botjes hun doel te bereiken. Een botje is een programma dat achtereenvolgens bij vele websites probeert binnen te dringen.
Dagelijks wordt iedere website door tientallen tot duizendtallen botjes bezocht. Deze zijn niet allemaal schadelijk: ze worden onder andere door zoekmachines gebruikt om de webpagina's te inventariseren.

Conclusie

Denk niet dat jouw website zo onbelangrijk is dat deze niet gehackt zal worden. Juist van veel 'onbelangrijke' websites is de beveiliging niet in orde en daardoor zijn ze een eenvoudig doelwit.
Kortom: het is nodig om de beveiliging van jouw website regelmatig te heroverwegen. Hackers ontwikkelen steeds nieuwe technieken, mede op basis van gevonden veiligheidslekken. Ze weten dat niet iedereen de laatste versie van de programmatuur installeert. Dus wordt gekeken of daar misbruik van kan worden gemaakt.
Controleer ook regelmatig of jouw CMS nieuwe plug-ins/modules heeft om je website veiliger te maken!

https://nl.wikipedia.org/wiki/Man-in-the-middle-aanval