Software updates

WordPress brengt gemiddeld om de 2 maanden een update uit. Gewoonlijk om bugs en verschillende beveiligingsproblemen op te lossen. Updates voegen ook nieuwe functies en functionaliteit toe die het algemene ontwerp en de prestaties van uw site kunnen verbeteren. De belangrijkste componenten die regelmatig moeten worden bijgewerkt, zijn de WordPress-core, thema's, plug-ins en andere software die uw site ondersteunt zodat alles soepel blijft lopen.

Plugin Management

Plug-ins zijn onafhankelijke stukjes software die zijn ontworpen door verschillende ontwikkelaars buiten WordPress. Wanneer WordPress updates voor zijn kernsoftware uitgeeft, is het de verantwoordelijkheid van de ontwikkelaar om hun plug-ins up-to-date te houden. Daarom is het belangrijk om, voordat we ervoor kiezen om een plug-in te installeren, de plug-in te onderzoeken, reviews te lezen en de laatst uitgevoerde updates te controleren. Eenmaal geïnstalleerd, is het belangrijk om door te gaan met het bijwerken van de plug-in terwijl ontwikkelaars updates uitvoeren voor compatibiliteit met WordPress.

Softwareconflicten

Hoewel het mogelijk is om de updates zelf uit te voeren, is het behoorlijk tijdrovend en riskant om het goed te doen. Het is belangrijk om regelmatig updates te laten uitvoeren door een professionele ontwikkelaar die weet wat hij doet en eventuele problemen die uit de update kunnen voortvloeien, kan volgen en aanpakken. Software-updates verlopen meestal soepel, maar soms botsen ze met elkaar en kunnen ze leiden tot storingen die een slechte ervaring voor uw bezoekers kunnen veroorzaken, of erger nog, maar uw site volledig naar beneden halen. (Ahhh!)

Veiligheidsproblemen

Een andere reden waarom het belangrijk is dat een professional consistent WordPress-onderhoud uitvoert, is het voorkomen van mogelijke inbreuken op de beveiliging. Wanneer updates worden geïnstalleerd, zijn er wijzigingen in uw bestanden waardoor uw site kwetsbaar is voor aanvallen van hackers. Onderdeel van het onderhoudsproces dat GeniusApps met WordPress uitvoert, zijn consistente back-ups van uw site. Back-ups worden ook uitgevoerd voordat updates worden gemaakt. Back-ups gaan tot 3 maanden terug en derhalve kunnen we altijd een goede back-up terug plaatsen. Elke op CMS (Content Management System) gebaseerde website is kwetsbaar voor aanvallen van hackers. Door uw WordPress-website-kern, plug-ins en thema's up-to-date te houden, voorkomt u dat uw website kwetsbaar is voor malware-infecties en externe aanvallen.

Denk je dat je site geen doelwit is voor hackers?

"Oh, ik ben maar een kleine jongen, niemand heeft een reden om mijn website aan te vallen." Dit is een veel voorkomende misvatting over de beveiliging van websites en de noodzaak van onderhoud. Te vaak zetten website-eigenaren onderhoud op een laag pitje omdat ze een kleine website hebben of niet denken dat iemand reden zou hebben om informatie van hun site te stelen. Maar als updates worden genegeerd, bent u een belangrijk doelwit voor kwaadaardige aanvallen.

Voor hackers gaat het niet om het stelen van informatie, maar om het kapen van uw site om de server te gebruiken als een hosting omgeving om spam-e-mails te verzenden of andere servers aan te vallen. Hackers maken vaak bots om kwetsbare sites te zoeken. Zodra een toegangspunt is gedetecteerd, komt de hacker binnen en neemt de controle over de server over.

De server wordt vervolgens gebruikt om spam naar enorme e-maillijsten te sturen. Dit zal de reputatie van uw site bij zoekmachines beschadigen en hen ertoe aanzetten uw IP-adres te blokkeren, waardoor uw site vrijwel onbestaande wordt in zoekresultaten. Hacks kunnen lange tijd sluimeren, terwijl de hacker andere websites infecteert en een leger van uitgebuite servers bouwt, "botnets" genoemd.

Hackers gebruiken geïnfecteerde servers om een DDoS-aanval (Distributed Denial of Service) op andere netwerken uit te voeren. Botnets sturen een zwerm spambots om andere sites te infecteren, phishing in te stellen en / of DDoS-aanvallen te vergemakkelijken. Dit type aanval is bedoeld om controle te krijgen over meerdere services, wat eenvoudig kan worden bereikt met een botnet.

Algemene website-onderhoudstaken:

Dit zijn enkele van de belangrijkste onderhoudstaken die op uw site moeten worden uitgevoerd.

WordPress Core Updates

WordPress zelf is een snel bewegend platform en nieuwe functies worden toegevoegd en regelmatig verbeterd. Als de WordPress Core niet up-to-date is, wordt uw website geleidelijk minder veilig en stabiel en zal deze niet presteren op het niveau dat het zou moeten zijn. Dit kan niet alleen een slechte ervaring voor uw bezoekers veroorzaken, het kan ook een negatieve invloed hebben op de rankings van zoekmachines.

Thema-updates:

Thema's vormen het raamwerk dat uw site eruit laat zien en doet wat hij doet. Net als de WordPress Core worden thema's vaak verbeterd en bijgewerkt voor

beveiliging en prestaties. Het gebruik van een verouderd thema beperkt de functie, beveiliging en vorm van uw aanwezigheid op het web.

Plugin Updates:

Plug-ins zijn de tools die aan uw WordPress-site kunnen worden toegevoegd om functies toe te voegen en de functionaliteit ervan te vergroten. Er zijn veel verschillende plug-ins beschikbaar om u te helpen alles te doen, van het maken van formulieren tot het toevoegen van visuele effecten. Plug-ins worden door verschillende auteurs gemaakt en regelmatig bijgewerkt. Als de auteur uw plug-ins bijwerkt, maar deze niet op uw website zijn geïnstalleerd, loopt u mogelijk verbeterde functies mis of veroorzaakt u beveiligingsproblemen en storingen op uw website.

Off-site back-ups:

Het WordPress-platform is stabiel, maar dat betekent niet dat het onoverwinnelijk is. In het geval dat uw website wordt gehackt of om een of andere reden uitvalt, kan het hebben van een back-up off-site (op een externe server) u beschermen tegen de verwoestende effecten van helemaal opnieuw moeten beginnen. Offsite back-ups van uw website moeten vaak worden gemaakt, vooral omdat u steeds meer nieuwe inhoud plaatst.

Beveiliging en bescherming:

Beveiliging wordt echter niet licht opgevat door WordPress, zelfs als het platform wordt versterkt; kwaadwillende individuen zullen nieuwe manieren verkennen om ze te overwinnen. Een ding dat de meeste website-eigenaren niet weten, is dat Google en andere zoekmachines een met malware geïnfecteerde website daadwerkelijk op de zwarte lijst plaatst, waardoor deze vrijwel onzichtbaar in het zoekverkeer wordt. Waarom?

Omdat een gehackte website een beveiligingsrisico is voor hun gebruikers en voor andere websites. Het zorgt voor de verspreiding en escalatie van malware-aanvallen op andere websites, en zelfs aanvallen op nationale doelen en infrastructuur. Ervoor zorgen dat uw beveiliging up-to-date en op zijn best is, is zeker iets dat serieus moet worden genomen.

Het begrijpen van de kwetsbaarheden en het nemen van de nodige voorzorgsmaatregelen is van vitaal belang voor de bescherming van uw website en mogelijk de reputatie van uw merk.

Verbroken koppeling Inspectie & reparatie:

Wanneer mensen op een website problemen tegenkomen zoals dode links, kan dit een grote turn-of-turn zijn. Dode links sturen een bericht naar uw bezoekers dat u

niet genoeg om uw site geeft en dat u waarschijnlijk niet voor andere zakelijke correcte verwijzingen zorgt, inclusief uw klanten. Door regelmatig gebroken links te scannen en op te lossen, kunt u ervoor zorgen dat uw bezoekers gemakkelijk door uw site kunnen navigeren en niet gefrustreerd raken en wegrennen naar uw concurrenten.

Dode links kunnen je ook pijn doen met zoekranglijsten. Wanneer zoekmachines meerdere verbroken koppelingen op uw site tegenkomen, geeft dit aan dat uw site verouderde inhoud van lage kwaliteit bevat en daarom niet de beste plek is om naar hun gebruikers te sturen voor goede informatie.

Ongebruikte plug-ins verwijderen:

Hoewel het onschadelijk kan lijken, moet inactieve of ongebruikte software op uw site worden vermeden. Misschien had je op een gegeven moment die agenda-plug-in nodig, maar gebruik je nu een andere, zodat die oude geïnstalleerd kan conflicten veroorzaken en de snelheid en functionaliteit van je site belemmeren. Het doornemen van uw plug-ins en het verwijderen van de plug-ins die niet nodig zijn, is een verstandige onderhoudsbeurt om het risico op een website-crash of storing te verminderen. Toch hoeft u zich niet over plug-ins te buigen, wij kunnen u vanuit onze onderhoudspakketten ontzorgen hierin.

Spam-opmerkingen verwijderen:

Een blog op uw WordPress-site kan een uitzonderlijke methode zijn om verkeer te genereren en uw merkimago op te bouwen. Reacties op uw blogs kunnen ook van grote waarde zijn om extra informatie te geven en discussie te genereren over onderwerpen die belangrijk zijn voor uw bezoekers. Helaas, net als e-mail, kunnen reacties op reacties worden gebruikt als middel om te spammen. Als de opmerkingen zichtbaar zijn voor andere bezoekers, kan je reputatie snel naar het zuiden gaan. Als u de tijd neemt om die spam-opmerkingen te verwijderen, blijven uw bezoekers tevreden en betrokken.

Conclusie

Dat zijn slechts enkele van de vele onderhoudstaken die op elke site belangrijk zijn. (Niet alleen WordPress). We bieden totaal ontzorgd pakketten aan onze klanten omdat we willen dat ze het maximale halen uit de sites die we voor hen bouwen, en we willen onze websites kunnen laten zien aan toekomstige klanten. Een goed onderhouden website laat ons er goed uitzien en onze klanten zien er ook goed uit. Meer informatie over deze totaal ontzorgd pakketten:

https://geniusapps.nl/prijzen-totaal-ontzorgd-abonnement-onderhoudscontract/

Wilt u meer zekerheid? De meeste van onze klanten kiezen voor het pakket C. Een bijkomend voordeel is dat u kunt rekenen op onbeperkte persoonlijke support.