5 supertips voor een betrouwbare en veilige website

Je website is cruciaal voor je bedrijf

Je website is een van de belangrijkste onderdelen van je bedrijf. Het is van vitaal belang dat je deze up-to-date, beschermd en online houdt, zodat deze beschikbaar is voor je klanten.

Als je website offline is of last heeft van problemen, is hij niet langer effectief voor je bedrijf. Sterker nog: een website die offline is, zorgt voor omzetverlies door verloren bezoekers of reputatieverlies.

Vandaag de dag zijn er meer factoren waar je je bewust van moet zijn. Een gemiddelde website is dagelijks gemiddeld een aantal keren doelwit van een al dan niet geautomatiseerde hackpoging,

Zorgt je goed voor je WordPress-website? Wanneer heb je voor het laatst updates uitgevoerd in het admin-dashboard? Misschien heb je zelfs wel nooit ingelogd in de back-end van je WordPress-website.

Je website draait met behulp van software, net als je PC, Mac, laptop, tablet of mobiel apparaat. Als je die software niet up-to-date houdt, loop je het risico op fouten, storingen of in het ergste geval malware-infecties.

Aandacht besteden aan updates, ervoor zorgen dat deze effectief worden uitgevoerd op je website en het testen ervan kost wel tijd. Tijd die je misschien niet hebt, maar het is een cruciale taak omdat het je website veilig, online en zichtbaar zal houden voor je (potentiële) klanten.

Heb je iemand in je bedrijf die voldoende kennis heeft van WordPress om deze updates uit te voeren? Het is niet raar als dat niet zo is. Een medewerker te hebben met de juiste vaardigheden om voor je website te kunnen zorgen kan zomaar € 30.000 per jaar kosten. Maar je moet wel een plan hebben om je website up-to-date en veilig te houden.

In deze gids geef ik je vijf belangrijke stappen, om je te helpen een onderhoudsschema op te stellen en je website veilig te houden. Het nemen van deze stappen geeft je gemoedsrust en stelt je in staat om je te concentreren op wat belangrijk is voor je bedrijf.

1. Peace Of Mind - Laat back-ups niet aan het toeval over

Een van de ergste dingen die jou als ondernemer kan overkomen, is dat je erachter komt dat je website offline is. Of erger nog, als je een e-mail krijgt van een klant die je vertelt dat je website offline is. Of dat Google je website aanmerkt als onveilig, door malware.

Wat doe je in zo'n situatie? Voor de meeste mensen zou dit betekenen dat je je hostingbedrijf belt en dat je vervolgens volledig afhankelijk bent van het vermogen van hun supportteam om je te helpen. Vaak zullen ze in staat zijn om een back-up van je website te herstellen - maar het kan zijn dat deze niet alle laatste gegevens bevat, vooral als je je website regelmatig bijwerkt of als er nieuwe bestellingen hebben plaatsgevonden.

Als ondernemer is het belangrijk dat je een noodplan hebt. Als je dat nog niet hebt, moet je nu een moment nemen en nadenken over wat je gaat doen als er iets mis gaat met je website.

Het belangrijkste onderdeel van je noodplan draait om het hebben van goede back-ups. Met een goede volledige back-up van je website kun je je website op ieder moment opnieuw in de lucht brengen, zelfs bij een andere hostingprovider als dat nodig is.

Er zijn drie belangrijke dingen waar je over na moet denken rondom je back-ups:

1. Off-site Back-up - Voor een goede beveiliging en veiligheid moeten je back-ups worden opgeslagen bij een externe dienst. Bijvoorbeeld - Amazon S3, Google Drive of Dropbox. Daarmee zorg je ervoor dat ook beschikt over je back-ups als je huidige hostingprovider onbereikbaar is.
2. Back-up schema - Je back-up schema zal afhankelijk zijn van hoe vaak je je website update en het type publiek dat je bedient. Voor de gemiddelde MKB WordPress website is een volledige back-up eenmaal per week en een dagelijkse database back-up vaak voldoende. Voor E-Commerce kan een dagelijkse volledige back-up en een dagelijkse database back-up een veel betere aanbeveling zijn.
3. Gecodeerd - Voor de veiligheid van je bedrijfsgegevens moet je een oplossing kiezen die de back-up van je website versleutelt voordat je deze off-site opslaat. Dit houdt jouw gegevens en vooral de gegevens van je klanten veilig.

TIP: Noteer de belangrijkste telefoonnummers of contactgegevens van je hostingbedrijf, domeinprovider en e-mailprovider. Als je problemen hebt met je website, moet je deze contactgegevens gemakkelijk bij de hand hebben. Zorg ervoor dat deze niet op dezelfde plaats blijven staan als je e-mails, want het is mogelijk dat je website en e-mails op hetzelfde moment down zijn.

2. Beveiliging - Goede beveiliging redt websites

Zoals ik in de inleiding van deze gids al zei, is een goede beveiliging van je website heel belangrijk voor je bedrijf.

Meer dan 30% van de websites op het internet draait op WordPress. Het is populair en zeer krachtig. Maar deze populariteit betekent ook dat je op je hoede moet zijn voor de veiligheid van je website.

Er zijn duizenden plugins die functionaliteit toevoegen aan WordPress websites. Een aantal van deze is geïnstalleerd op je website. Deze worden regelmatig voorzien van een functionele- en beveiligingsupdates. Ook de WordPress software wordt regelmatig geüpdatet.

De beveiliging van je website is jouw verantwoordelijkheid, als ondernemer. Je hostingbedrijf zal een aantal beveiligingsinstellingen hebben die helpen om je website te beschermen, maar deze zullen je niet beschermen tegen alle gevaren. Als er iets misgaat, kan je hostingbedrijf een back-up herstellen, zoals eerder genoemd, maar verder komt het waarschijnlijk op jou aan.

Je moet een goede beveiliging hebben op je WordPress website. Je kunt kiezen voor een gratis plugin, zoals WordFence of iThemes Security. Deze hebben allebei stappenplannen om je te helpen bij de installatie, maar je moet er wel voor zorgen dat je jezelf niet per ongeluk bij je eigen website buitensluit.

Wanneer je met derden werkt, zoals ontwikkelaars of ontwerpers, moet je altijd de volledige controle over alle wachtwoordinstellingen behouden. Dit betekent dat je je "masterwachtwoorden" (hoofdwachtwoorden) niet aan derden mag geven. Als iemand toegang tot je website, hostingaccount of een ander digitaal object nodig heeft, probeer er dan altijd voor te zorgen dat ze een unieke login hebben en dat deze op elk moment door jou of door je team kan worden uitgeschakeld.

Goede beveiliging is vooral een kwestie van je gezond verstand gebruiken. En een beetje geluk hebben. Geen enkele WordPress website is 100% veilig, in feite is geen enkele website ter wereld 100% veilig. De zwakke plek is in de meeste gevallen eigenlijk een mens - of het nu via scam of een gehackt apparaat is, of dat een iets slecht geprogrammeerd heeft.

TIP: Kijk eens terug op het afgelopen jaar en denk na over met wie je allemaal hebt samengewerkt. Heb je aan iemand van hen je hoofdwachtwoord gegeven? Heb je het daarna nog aangepast? Maak een lijst van alles waar je een wachtwoord van hebt gedeeld. Werk deze wachtwoorden dan bij met een sterk wachtwoord. Je kunt bijvoorbeeld https://strongpasswordgenerator.com gebruiken als je hulp nodig hebt bij het bedenken van een sterk wachtwoord.

3. Onderhoud – je website heeft nooit een vrije dag

Net als je auto heeft je website onderhoud nodig om in de beste conditie te blijven. Het is heel belangrijk dat er regelmatig onderhoud plaatsvindt aan je WordPress website.

Net als je auto heeft ook je website onderhoud nodig om in de beste conditie te blijven. Het is echt belangrijk dat er regelmatig onderhoud plaatsvindt aan je WordPress website.

Zonder regelmatig onderhoud loop je het risico dat je website wordt aangevallen, offline gaat door een fout of niet goed functioneert bij toekomstige updates.

Je zult regelmatig onderhoud moeten uitvoeren, of uit laten voeren.

Wat moet je dan doen? Hier is een lijst van 4 belangrijke onderdelen van goed WordPress-onderhoud:

- **WordPress Updates** - Nieuwe versies van WordPress zijn periodiek beschikbaar. Deze zouden vrij snel geïnstalleerd moeten worden, omdat ze vaak veiligheidspatches bevatten.
- **Plugin Updates** - De plugins die in gebruik zijn op je website zullen regelmatige functie- en beveiligingsupdates beschikbaar hebben. Deze zouden vaak geüpdatet moeten worden, om er zeker van te zijn dat alles veilig is.
- **Thema Updates** - Het thema dat in gebruik is op je website zal ook regelmatig updates beschikbaar hebben. Zorg ervoor dat je je thema update om je website veilig te houden.
- **Controleer Back-ups** - Je moet controleren of je proces rondom je back-ups goed loopt en of ze succesvol worden opgeslagen op een externe locatie. Back-ups zijn cruciaal!

Zorg er altijd voor dat je een recente back-up van je website hebt voordat je met het onderhoud van je website begint. Je moet je website terug kunnen draaien naar de vorige versie als je problemen hebt met de updates die je uitvoert.

TIP: Stel een onderhoudsschema op voor je website en hou je hier strikt aan. Hou hier ongeveer een uur per week voor vrij. Als je dit uitbesteed aan een van je medewerkers, zorg er dan voor dat hier alle benodigde middelen en tijd voor heeft, en vraag hem om voltooid werk te documenteren, zodat je hierop kunt terugkomen als je problemen hebt.

4. Betrouwbaarheid – hoe goed is je host?

Website hosting is een van de meest voorkomende digitale diensten die je online kunt vinden. Elke website heeft dat nodig. Zonder hosting zou je website niet zichtbaar zijn op het internet. Helaas biedt niet elk website-hostingbedrijf dezelfde kwaliteit en service.

Als je hosting op dit moment minder kost dan een kopje koffie per maand, dan is de kans groot dat je te weinig betaalt. Low-cost hosting is op een zogenaamde "shared environment", een gedeelde server. Hierbij worden duizenden websites op dezelfde server geperst. Het voordeel voor het hostingbedrijf is dat ze aan elke server meer geld kunnen verdienen, maar dit is natuurlijk niet gunstig voor jouw website.

Wanneer je website op een gedeelde hostingserver staat, deel je dezelfde resources met duizenden andere websites. Als een van deze websites de beschikbare resources in beslag neemt of een actie uitvoert die een probleem op de server veroorzaakt, kan je website offline gaan.

Prestatieproblemen kunnen een belangrijke factor zijn op een gedeelde hostingomgeving. Bezoekers van je website zullen gemiddeld zo'n 5 seconden wachten voordat ze zich vervelen en elders gaan kijken. Als je website langzaam inlaadt, naar welke concurrent denk je dan dat ze gaan?

Een ander punt wat je aandacht is verdient is je e-mail. Als je je e-mails en je website bij dezelfde hostingprovider host, worden je e-mails allemaal vanaf dezelfde server verstuurd, net als vele duizenden andere e-mailadressen. Als slechts één persoon op de server besluit om veel spam te gaan versturen, bewust of niet, kan dit ertoe leiden dat het IP-adres van de server wordt geblokkeerd door e-mailproviders. Als dit gebeurt, dan betekent dat dat ook jouw e-mails niet worden afgeleverd bij je klanten, leveranciers en andere belangrijke ontvangers. Een groot probleem, natuurlijk!

E-mails moeten extern worden gehost op je website. Bekijk G Suite, Office 365 of Zoho Mail voor betaalbare e-mailoplossingen.

In deze digitale tijd zou je als ondernemer niet moeten bezuinigen op je hosting. Een schatting: uitstekende hosting voor een gemiddelde website kost tussen de € 20 en € 25. Ja, dit is meer dan een kopje koffie. Maar wat kost het om website met problemen door goedkope hosting te repareren? Dat loop al snel in de honderden euro's.

TIP: Bekijk hoeveel je momenteel betaalt voor je hosting. Als je voor je hosting per maand hetzelfde betaalt als één of twee kopjes koffie, dan is de kans groot dat dit hostingpakket niet de beste optie voor je is. Kijk ook eens serieus naar je e-mail. Overstappen naar G Suite kost ongeveer € 5 per maand per gebruiker. G Suite is een van de meest betrouwbare e-mailplatforms op het internet - gerund door Google.

5. Wees proactief. Wacht niet tot het fout gaat

Wil je proactief zijn, je website up-to-date houden, klaar zijn voor eventuele problemen die zich voordoen? Of wil je liever reactief zijn en alleen reageren als er een probleem is, en het meestal al veel te laat is voor een snelle oplossing?

Als ondernemer wil je natuurlijk op de kosten letten, maar bedenk je wel dat het is veel duurder om te reageren op een ramp dan om goede voorzorgsmaatregelen te treffen om problemen te voorkomen.

Heb je de vaardigheden om voor je website te zorgen of heb je een ervaren medewerker in dienst? Zoals ik in de inleiding van deze gids al schreef, kunnen de kosten voor een goede WordPress-medewerker al snel in de buurt van € 25.000 per jaar liggen. Dat is nog exclusief sociale lasten en een extra werkplek in je bedrijf.

Natuurlijk kan deze medewerker ook part-time in dienst nemen, maar dan moet je er wel op kunnen vertrouwen dat hij beschikbaar is wanneer je hem nodig hebt.

En zelfs als je zelf de capaciteiten hebt om voor je eigen website te zorgen, heb je daar dan de tijd voor? Het kost je ongeveer een uur per week, maar als er een probleem ontstaat dat je onmiddellijke aandacht nodig hebt, kan dit zomaar nog eens 2 tot 4 extra uur duren. Zou je die tijd niet veel liever besteden aan andere zaken in je bedrijf?

Het is oké dat je het druk hebt. Je hebt als ondernemer elke dag veel belangrijke taken te vervullen en dat is volkomen begrijpelijk. Het is goed dat je het druk hebt, want het betekent dat je bedrijf het goed doet.

Er is een andere optie: je kunt het voordelig uitbesteden. Zo bied ik WordPress Super Service: een dienst waarbij ik de zorg voor je website helemaal van je overneem. Ik zorg ervoor dat deze up-to-date en veilig blijft en dat er altijd goede back-ups zijn van je gegevens. Met WordPress Super Service hoef je je nooit meer zorgen te maken over je website en kun je je te concentreren op de belangrijkere taken die je nodig hebt, elke dag opnieuw. Nooit meer WordPress Stress.

TIP: Hoeveel kost het als je minstens 4 uur met maand moet besteden aan het onderhoud van je website? Of als je daar een medewerker voor zou moeten aannemen? Is er ook een training nodig voor deze medewerkers om WordPress onderhoudstaken uit te kunnen voeren? Als het totaal meer dan € 40,- per maand bedraagt, dan ben je financieel beter af met een WordPress Super Service voor je bedrijf.

Neem geen risico's met je website

Het kan spannend zijn om risico’s te nemen op een racebaan of als je aan een pokertafel zit, maar met je website moet je zoveel mogelijk risico’s uitsluiten. Er is altijd wel een geautomatiseerd script of een vastberaden hacker die jouw website heeft aangemerkt als zijn volgende slachtoffer.

Je vraagt je misschien af waarom iemand jou website zou willen hacken. Je bent toch geen grote, bekende website? Goede vraag.

Aanvallen op websites gaan tegenwoordig niet alleen over het stelen van gegevens. Veel aanvallen kunnen ook gericht zijn op het gebruik van je website om spam-e-mails te verzenden of schadelijke inhoud toe te voegen die is ontworpen om de reputatie van een andere website te verbeteren.

Misschien heb je geen probleem gehad sinds de lancering van je website, misschien ben je wel een van de gelukkigen die nog nooit een websiteprobleem hebben gehad, maar wat gebeurt er als het je eerste keer is?

De eerste stap die je kunt nemen om de grootse toekomst van je website veilig te stellen, is dat je vandaag de tijd neemt om je noodplan op te stellen goed op een rijtje te zetten met wie je contact moet opnemen als er iets misgaat.

Door je te concentreren op deze 5 tips, kun je je website en je bedrijf vooruit helpen.

Ik heb nog enkele aanvullende tips en ideeën die ik je de komende dagen zal sturen, met wat extra inzichten over de bovenstaande onderwerpen.

Als je in de tussentijd vragen hebt of meer wilt weten over een onderwerp in dit gratis e-book, neem dan zeker contact op.

Ik wens je een fijne dag!

06 – 288 397 41

rick@bureauram.nl

bureauram.nl