Vernieuwde AVG

Ben jij er klaar voor?

Best4ugroup

Ben jij klaar voor de AVG?

Online veiligheid en de bescherming van persoonsgegevens zijn actuele onderwerpen. 'Het internet' heeft steeds meer gegevens van burgers in handen en ondertussen groeit de wereldwijde dreiging van cybercriminaliteit. Om persoonsgegevens beter te beveiligen is vanaf mei 2018 de Algemene Verordening Gegevensbescherming van kracht. Voor ondernemers betekent dat strenge wetgeving en belangrijke maatregelen! Ben jij klaar voor de vernieuwde AVG?

Vanaf 25 mei 2018 geldt voor heel Europa de nieuwe privacywetgeving. De General Data Protection Regulation (GDPR) vervangt de Wet bescherming persoonsgegevens en legt bedrijven extra plichten op. Voldoet jouw bedrijf hier vanaf 25 mei 2018 niet aan, dan riskeer je flinke boetes. Hoog tijd voor actie!

Het uitgangspunt van de AVG voor ICT bedrijven is dat de betrokkene (dat is jouw klant) te allen tijde beschermd moet worden. Dat houdt in dat je alle gegevens die je van jouw klant opslaat moet beveiligen. Mocht je onverhoopt te maken krijgen met een datalek (bijvoorbeeld wanneer je website wordt gehackt) en je maakt hier geen melding van bij de Autoriteit Persoonsgegevens, dan riskeer je een boete die 4% van je totale jaaromzet kan bedragen.

Wat nu?

De AVG geldt voor elke ondernemer en dus ook voor het MKB. Omdat de regels flink worden aangescherpt is het belangrijk om op de hoogte te zijn van de eventuele aanpassingen die voor jouw bedrijf van belang zijn. Bij Best4u weten we dat in principe ieder online product gevaar loopt. Cybercriminelen slaan hun slag en brengen schade toe middels ransomware, malware, SQL injecties en DDoS-aanvallen. Ook jouw website - en dus de persoonsgegevens van klanten die jij middels je website verzamelt - ontlopen zonder de juiste tegenmiddelen het vizier van de cybercrimineel niet.

In deze whitepaper lichten we vier belangrijke stappen toe die in elk geval van belang zijn in het kader van de AVG. Ook geven we geven je een kijkje in de maatregelen die wij voor onze klanten nemen, zodat zij met een gerust hart kunnen ondernemen.

Vier belangrijke stappen

Stap 1: Breng in kaart over welke gegevens je beschikt

De nieuwe privacywet geldt voor alle gegevens die jij (ooit) hebt verzameld en opgeslagen van klanten. Dat kan variëren van ingevulde contactformulieren tot een Word-document met adresgegevens. Het is daarom verstandig om als eerste stap in kaart te brengen over welke gegevens jouw bedrijf allemaal beschikt en vervolgens te bekijken waar al die gegevens zijn opgeslagen.

Stap 2: Verwerkersovereenkomst opstellen

Als je in kaart hebt gebracht over welke gegevens je beschikt en waar je deze opslaat, is het tijd om je met verwerkersovereenkomsten bezig te houden. Deze overeenkomsten sluit je met de bedrijven die in opdracht van jou gegevens opslaan. Werk je bijvoorbeeld met een extern CRM of met een websitebeheerder, dan moet je ervoor zorgen dat je met deze bedrijven een overeenkomst hebt. In deze overeenkomst staat wat de verwerkers mogen doen met de gegevens die zij voor jou opslaan en hoelang zij deze gegevens mogen bewaren.

Best4u is ook verwerker. Onze verwerkersovereenkomst staat vermeld in onze Algemene Voorwaarden.

Stap 3: Privacyverklaring aanpassen

In je privacyverklaring beschrijf je (in grote lijnen) waar je bedrijf voor staat, welke persoonsgegevens het bedrijf verwerkt en hoe bereikbaar het bedrijf is.

Algemeen - In een goede privacyverklaring is beschreven welke uitgangspunten op gebied van privacy nagestreefd worden, welke maatregelen er genomen worden voor persoonsgegevensbescherming en op welke datum dit document voor het laatst is aangepast. Ook wordt hierin benoemd of er een privacy manager is en hoe die te bereiken is. Daarnaast zijn de contactgegevens van het bedrijf vermeld.

Persoonsgegevens - Welke gegevens wil je bewaren, waarom bewaar je deze gegevens, waar bewaar je die gegevens en voor hoelang blijven deze gegevens bewaard? Deze punten moeten allemaal duidelijk naar voren komen in de privacyverklaring. Wil je bijvoorbeeld het e-mailadres van iemand die ooit een whitepaper van jouw website heeft gedownload gebruiken voor een nieuwsbrief, dan moet dit in je privacyverklaring vermeld staan.

Bereikbaarheid - De AVG is in het leven geroepen om de bescherming van persoonsgegevens van betrokkenen (bijvoorbeeld klanten van webshops) te verbeteren. De relatie tussen betrokkenen en de organisaties die gegevens van hen verwerken is dus in het voordeel van de betrokkenen versterkt. Dat houdt in dat organisaties ervoor moeten zorgen dat betrokkenen de rechten die zij hebben bij die organisatie kunnen ‘inwilligen’. Ook over de klachtprocedure en de mogelijkheid tot contact in het kader van deze rechten moet geïnformeerd worden in de privacyverklaring.

Stap 4: Gegevens veilig opslaan

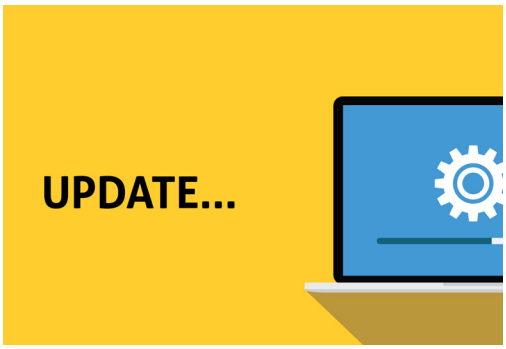
Dit lijkt een open deur, maar wees je bewust van het feit dat alle gegevens waarover jij beschikt veilig opgeslagen moeten worden. Jouw klanten geven namelijk geen toestemming om de gegevens die jij van hen hebt ontvangen ook aan een ander te laten zien of voor andere doeleinden te gebruiken. Het is daarom van belang dat je er zeker van bent dat alleen jij en je websitebeheerder in je website kunnen inloggen in je website. Ook een document met e-mailadressen dat ergens op je computer ‘rondzwerft’ moet beveiligd worden.

Best4u's cybersecurity oplossingen

Naast de vier belangrijke stappen om te voldoen aan de AVG vertellen we je ook graag meer over de maatregelen die wij nemen op het gebied van cybersecurity. Met deze maatregelen beschermen wij de websites van onze klanten, zodat zij wat de bescherming van persoonsgegevens betreft weer sterker staan. Hieronder lichten we de volgende onderdelen toe:

- Updates
- Back-ups
- Plugins
- SSL
- Monitoren & scannen
- Aanvallen op serverniveau
    - Verkeer analyseren
    - Maleware herkennen
    - DDoS protectie
    - 24/7 Managed

Updates



WordPress is een open source CMS. Dit houdt in dat ontwikkelaars niet alleen regelmatig nieuwe plugins ontwikkelen, maar ook dagelijks bezig zijn met het ontwikkelen van updates voor het systeem op het gebied van veiligheid, snelheid en gebruiksvriendelijkheid. Die updates moeten doorgevoerd worden om te zorgen dat een website optimaal blijft functioneren. Een WordPress website die niet onderhouden wordt zal uiteindelijk gebruikt worden door hackers om spam de wereld in te sturen met jouw website als afzender. Ook kunnen hackers je website offline halen, vreemde tekens plaatsen of extra pagina's aanmaken met reclame over zaken als viagra. Dit wil je als bedrijf zijnde vanzelfsprekend niet. Echter is klakkeloos op de update-knop klikken niet verstandig. Het kan er zelfs voor zorgen dat je website offline gaat.

Best4u voert daarom vóór elke update eerst een risicoanalyse uit. Hierbij wordt gekeken naar de nieuwe informatie die aangeboden wordt en of die informatie wel veilig is voor de website. Pas als de eventuele risico's in kaart zijn gebracht, kan een website veilig geüpdatet worden.

Back-ups

Stel; onverhoopt wordt je website toch gehackt, hij crasht tijdens het updaten van WordPress of een plugin of je hebt een fout gemaakt. Een back-up zorgt er in zulke gevallen voor dat je website snel weer online is. Wij raden daarom aan om dagelijks een back-up van je website te maken. Dit kan op verschillende manieren binnen WordPress. De meeste mensen zijn hier echter niet van op de hoogte. Daarom bieden we jou bij Best4u een back-updienst aan. Op die manier weet je zeker dat, mocht er onverhoopt iets misgaan, je altijd beschikt over een back-up die wij voor je terug kunnen zetten. Zo ben je in noodgevallen dus snel weer online.

Plugins

Een ander gevaar wordt gevormd door het downloaden van plugins. Middels plugins kun je functionaliteiten aan je website toevoegen. Officieel bestaan er voor WordPress bijna 52.000 plugins en daarbuiten bestaan er nog eens duizenden onofficiële varianten. Plugins kunnen je website fantastisch uitbreiden en aanvullen, maar ook hierbij is een check noodzakelijk. Het is namelijk nooit helemaal voorspelbaar hoe een plugin interacteert met een thema of met een andere plugin. Ook is het een risico om oude software rechtstreeks te updaten als je al enkele nieuwere versies hebt overgeslagen.

Om deze risico's van het updaten van WordPress te onderkennen, mogelijke problemen op te kunnen lossen of een oudere versie van de website terug te kunnen zetten is enige kennis van CSS, HTML, MySQL, PHP, de beheeromgeving (bijv. directadmin of cPanel), phpMyAdmin en FTP vereist. Het is daarom verstandig om plugins die je op je website wilt door Best4u te laten installeren.

SSL

Een SSL certificaat zorgt voor zichtbare beveiliging van je website. Met een SSL certificaat versleutel je het dataverkeer tussen de browser en de server zodat vertrouwelijke gegevens worden beschermd en niet kunnen worden onderschept. Websites met een SSL certificaat zijn te herkennen aan het groene slotje in de adresbalk. Bij Best4u voorzien we websites die bij ons gehost worden standaard van een SSL certificaat.

Monitoren & scannen

Het up-to-date houden van je WordPress website is een belangrijke eerste stap om de beveiliging van je website te versterken. Er zijn daarnaast nog veel meer maatregelen die ervoor zorgen dat kwaadwillenden jouw website niet zullen ‘misbruiken’. Door je website te monitoren en regelmatig malware scans uit te voeren houden wij de veiligheid van je website goed in de gaten. Wij gebruiken de CXS malware scanner om bestanden van de server te scannen op malware.

Een gehackte website kost geld en tijd, maar daarnaast kun je ook nog eens op de zwarte lijst van Google terecht komen. Hierdoor wordt je website praktisch onvindbaar op het internet. Om dit te voorkomen (en snel op te kunnen lossen) is het monitoren en scannen van je website onmisbaar.

Aanvallen op serverniveau

Bij Best4u zijn we verantwoordelijk voor een zeer groot aantal live websites. Deze websites draaien allemaal op servers die op vrijwel elk moment van de dag meerdere aanvallen tegelijkertijd moeten verwerken. Ook op serverniveau moeten wij dus continu aanvallen detecteren en blokkeren. Deze aanvallen zijn divers, maar wel te categoriseren in groepen en maatregelen en in de belangen van de initiator. Vaak wil de initiator met de aanval bekende zwakheden zoals verouderde software en veel voorkomende wachtwoorden achterhalen.

Onze servers worden beheerd door managed hosting partner Rootnet. Onder andere met de volgende maatregelen zorgen zij er in samenwerking met ons voor dat aanvallen op serverniveau gedetecteerd en geblokkeerd worden.

Verkeer analyseren

Door het verkeer naar websites te analyseren met behulp van software houdt Rootnet in de gaten of er herkenbare patronen voorkomen in dat verkeer. Een herkenbaar patroon kan bijvoorbeeld voorkomen als een computer wachtwoorden blijft uitproberen op een loginpagina van een website. De betreffende computer (het IP-adres) wordt dan voor enige tijd tegengehouden via een firewall. Hiermee is de aanval automatisch afgevallen. Middels deze techniek worden er per minuut enkele tientallen nieuwe computers/IP-adressen geblokkeerd.

Malware herkennen

Rootnet beschikt over een database met meer dan 100.000 eerder herkende malware of virussen. Elk nieuw bestand dat aangemaakt wordt op de server, zoals een toegevoegde foto of uitbreiding van een pagina, wordt razendsnel gescand om te checken of er patronen in het bestand voorkomen die overeenkomen met een virus of malware in de database. Bij herkenning wordt Best4u gewaarschuwd. Wij zullen het bestand dan nader onderzoeken en indien nodig direct verwijderen.

DDoS protectie

DDoS (Distributed Denial Service Attack)-aanvallen zijn aanvallen waarbij honderden computers tegelijkertijd dezelfde website(s) aanroepen. Kort gezegd is de server dan zo druk met het verkeer naar die website dat al het andere verkeer naar die server plat gelegd wordt. Rootnet zet meerdere defensieve technieken in om dergelijke aanvallen te detecteren en te voorkomen.

Eén van die technieken maakt het mogelijk om bij herkenning van een DDoS aanval al het internetverkeer naar een server om te leiden via een ‘wasstraat’. In die ‘wasstraat’ staat gespecialiseerde apparatuur van verschillende fabrikanten die het internetverkeer ontdoen van DDoS verkeer, waarna het verkeer alsnog zal worden doorgestuurd naar de server. Doordat dit omschakelen tijdens een aanval automatisch verloopt en slechts enkele seconden duurt merken gebruikers van websites vaak nauwelijks iets van een dergelijke aanval.

24/7 Managed

24 uur per dag is er monitoring actief en worden er tientallen punten gemeten op onze servers. Worden er afwijkingen gedetecteerd, dan ontvangt een engineer van Rootnet een signaal. Op die manier kunnen aanvallen die niet automatisch herkend worden alsnog in een vroeg stadium geblokkeerd worden. Aanvalstechnieken veranderen continu waardoor het altijd nodig blijft om servers 24/7 te managen en monitoren.

Meer weten?

Zorg er vandaag nog voor dat jouw bedrijf voldoet aan de regelgeving én dat jouw online product beschermd is tegen gevaren als DDoS aanvallen, malware en andere schadelijke praktijken. Laat je daarom adviseren door Best4u!

De support- en security experts van Best4u kunnen je nog veel meer vertellen over de maatregelen die nodig zijn om jouw online product te beschermen. Neem gerust contact op met één van onze adviseurs via 0575 512 125 of mail naar support@best4u.nl.

Best4u group