Bescherming van de Amnesty servers en de daar gehoste websites van lokale Amnesty groepen

Table of Contents

Inleiding

Het webhosting team <webhosting@amnesty.nl> bestaat uit: Ed van Velzen, Han Koster en Richard Schlichting (bewerker van deze notitie, die in 2013 door Dick Diepen was opgesteld.)

Voor ons als webhosting team zijn / waren "hacks" van server en websites een harde leerschool.

Rond de hosting zijn daarom veranderingen doorgevoerd.

Ook de webmasters hebben in belangrijke mate invloed op de beoogde veiligheid.
Daarom zijn we genoodzaakt om expliciet een aantal voorwaarden te stellen bij de hosting op de Amnesty server.

"Vrijheid, blijheid" : Dat handhaven we, maar niet tot elke prijs.

De "content" van de websites blijft hier buiten beschouwing. Die wordt vanuit Amnesty gevolgd door het monitoring team. Er zijn geen overlappingen tussen beide teams. Wel vormen webhosting team en monitoring team samen de Amnesty InternetGroep.

In deze notitie bespreken we eerst :

- **Voorwaarden : wat we van jullie als webmasters verlangen**
- **Wat doet webhosting** -wat we zelf gedaan hebben en nog zullen doen.

De "voorwaarden": wat vragen we van de webmasters?

uitgangspunten

De technische kant (de "engine") van een website moet up-to-date en veilig zijn door het gebruik van recente en veilig te achten software op de server, en ook bij het gereedmaken van op de server te plaatsen bestanden.
Bij eventuele problemen moet de webmaster bereikbaar zijn voor overleg over oplossingen.

concrete uitwerking

Bereikbaarheid van de webmaster
- Zorg dat een persoonlijk e-mail adres van de webmaster bij het webhosting team bekend is. en geef altijd het nieuwe adres door bij een wijziging van het e- mail adres van de webmaster, of bij de overdracht van de functie.
- Gebruik een e-mail adres dat gebonden is aan de persoon van de webmaster, en niet een aan de website. Dus niet <webmaster@(groepsnaam).amnesty.nl> of <webmaster.(groepsnaam)@gmail.com> of zoiets.
- De webmaster is voor het webhosting team het primaire contact.
- De formele verantwoordelijkheid voor informatie over de webmaster blijft liggen bij de groep.

Specifiek voor "levende" websites (Joomla, Wordpress, andere php-sites)
wees terughoudend en prudent bij het installeren van extensies en plug-ins
Installeer geen overbodige uitbreidingen. Een aantal zaken wordt al standaard geïnstalleerd.
(Voor Joomla : zie bron.amnesty.nl)

Voor alle typen websites
- Verleen / handhaaf het webhosting team toegang tot de beheersomgeving (onder meer om de versie te kunnen monitoren en updaten)
- Waar die toegang niet of niet meer bestaat, zal het webhosting team hierover contact opnemen.

Gebruik een recente versie van alle software, CMS systeem, plug-ins en zo.

- Denk ook aan website-editor, tellers, foto-galerijen, gastenboeken, agenda's, php- en java-scripts, enzovoort.
- Overtuig je vooraf van de betrouwbaarheid van zowel de software als de distibuteur/leverancier. -
- Doe een verkenning op het web en/of vraag het na bij collega's of bij het hosting team

Meld storingen
- Een (al of niet vanzelf voorbijgaande) storing op een website kan onbelangrijk lijken.
- Wanneer meldingen over meerdere gelijksoortige storingen het webhosting team bereiken, is de kans groter dat er een patroon waarneembaar wordt. Dan is wellicht actie mogelijk.
- Meld dit liefst per e-mail, gericht aan het webhosting team, met tenminste vermelding van de website, een omschrijving van de aard van de storing en het moment waarop de storing is waargenomen.
- Meer gegevens zijn welkom, en waar relevant ook screenprints en/of de tekst van een storingsmelding.

Wat doet webhosting

- Preventie
- Bevoegdheden
- Beheer toegangscodes
- Database
- Hinder van preventieve maatregelen

Preventie

Er vonden en vinden nog steeds pogingen plaats om de server binnen te dringen.
Tot nu toe hebben we het volgende aan "bedreigingen"waargenomen:
- pogingen om een of meer websites te "kapen"
- pogingen tot misbruik voor eigen doeleinden van de mail-faciliteiten op de server
- pogingen van "bots" om vertrouwelijke informatie te verzamelen
- pogingen om zogenaamde "DDOS-aanvallen" voor te bereiden, bedoeld om een server "plat te leggen".

We blijven attent blijven op risico's en bedreigingen.
We moeten er immers van uit gaan dat er ook in de toekomst aanvallen blijven komen.

Een aantal preventieve maatregelen zijn al uitgevoerd. Enkele andere zijn nog in voorbereiding. Het zou niet van wijsheid getuigen om al die maatregelen hier te vermelden. We noemen hier enkele maatregelen die belangrijk zijn voor de webmasters.

- beschermende maatregelen
- strakker instelling van rechten op de servers.
- Versiebewaking Joomla!
- "Non-Joomla!" websites.
- Hinder van preventieve maatregelen

beschermende maatregelen
plaatsing van "beschermende bestanden" in alle webmappen
Voor een hacker maken deze bestanden het lastiger om daar zijn "malware" te plaatsen.

strakker instelling van rechten op de servers.
De schrijf- en toegangsrechten zijn beperkt tot wat strict nodig is om de website te kunnen onderhouden.
Dat betreft vooral “levende” websites. FTP verkeer is daar vervallen. Waar FTP verkeer noodzakelijk blijft, zoeken we zo veilig mogelijke alternatieven.

Versiebewaking Joomla!
De check of de Joomla!-versie en de extensies actueel zijn, is geautomatiseerd. Automatisch wordt gemeld dat update nodig is.
Zulke updates voeren we zo spoedig mogelijk uit. Daarom heeft het webhosting team toegang tot het beheersgedeelte.

"Non-Joomla!" websites.
Hier gaat het voornamelijk om (vrij summiere) extra bescherming door het op read-only zetten van start-bestanden.
En er is een zeg maar “speciale vervangende ftp met verhoogde veiligheidsborg” ingevoerd.

Van deze beschermende maatregelen hoor je als webmaster nu en in de toekomst niets te merken.

Hinder van preventieve maatregelen

Mocht je ooit het idee krijgen dat een probleem bij het functioneren of het onderhoud van "jouw" website verband zou houden met een actie van het webhosting team, neem dan direct contact op. Doe dat liefst per e-mail, gericht aan het webhosting team, met tenminste vermelding van de website, een omschrijving van de aard van de storing en het moment waarop de storing is waargenomen. Meer gegevens zijn welkom, waar relevant ook screenprints en/of de tekst van een storingsmelding.

Bevoegdheden van het webhosting team

- ingrijpen bij acuut risico
- ingrijpen bij storingen of ontoereikend onderhoud

ingrijpen bij acuut risico
- Bij een acuut risico voor de integriteit van de server, functies van de server of andere op de server ondergebrachte websites zal het webhosting team een afzonderlijke website gedeeltelijk of geheel off-line zetten of tijdelijk bepaalde functies van een website uitschakelen.

- Bij een acute en ernstige verstoring of bedreiging van het functioneren van de server zal het webhosting team dit doen zonder overleg vooraf. In andere gevallen zal eerst met de webmaster contact worden opgenomen, mits die webmaster bekend en binnen een redelijke termijn bereikbaar is, en in staat om op korte termijn de website weer aanvaardbaar te laten functioneren.

- Wanneer zo'n maatregel genomen wordt, zal hierover zo snel mogelijk ook een bericht gestuurd worden naar de contactpersoon van de groep, of anders naar de regio-coördinator.

ingrijpen bij storingen of ontoereikend onderhoud
- Wanneer een website storingen oplevert, technisch niet adequaat onderhouden wordt of anderszins niet goed functioneert zal het webhosting team dit bij de webmaster aan de orde stellen, en de website off-line zetten bij het uitblijven van tijdig herstel.

- Dit off-line zetten gebeurt ook wanneer de webmaster op het bij het team bekende adres niet voor overleg bereikbaar blijkt, en via de bij het team bekende contactpersoon ook geen contact mogelijk blijkt.

- Als de webmaster bereikt kan worden krijgt deze een redelijke termijn om het goed functioneren van de website alsnog te herstellen. Zo mogelijk wordt ook ondersteuning aangeboden. Wanneer het tot off-line zetten komt, wordt over deze maatregel zo snel mogelijk een bericht gestuurd naar de contactpersoon van de groep, of anders naar de regio-coördinator.

- Het als veiligheidsmaatregel maatregel off-line zetten van een website is in principe tijdelijk. Wanneer (weer) adequaat contact mogelijk is met de webmaster, zal het webhosting team zich inspannen om behulpzaam te zijn bij het weer op orde brengen van de website, dit om zo spoedig mogelijk weer een veilige en goed functionerende website on-line te kunnen zetten.

- Alleen wanneer overleg met webmaster en ook met de groep niet mogelijk blijkt, ook niet via de regio- coördinator, of wanneer dit overleg geen uitzicht biedt op voldoende herstel van de website, zal het webhosting team als uiterste maatregel een website van de server verwijderen.

- Het off-line of weer on-line zetten van een website leidt altijd ook tot een verzoek aan het webteam om de link naar de website op de regio-pagina op te schorten of te herstellen. Hiervan gaat steeds ook een bericht naar de contactpersoon van groep en naar de regio-coördinator.

Beheer van toegangscodes

- Het is mogelijk dat we besluiten om alle inlogcodes van tijd tot tijd te wijzigen.
- De beveiliging van "alles" op een server staat of valt voor een belangrijk deel met de manier waarop alle betrokkenen met wachtwoorden omgaan.
Wachtwoorden van "alle websites" zijn alleen bekend bij het webhosting team.

- Wachtwoorden van afzonderlijke websites dienen alleen bekend te zijn bij degenen die zich met de inrichting en het beheer van die website bezig houden, en verder eventueel ook nog bij een voor de continuïteit van een groep verantwoordelijke persoon.

- Mogelijk gaan we de toegangscodes voortaan standaard vervangen bij een wisseling van webmaster. Wachtwoorden zullen in elk geval vervangen worden indien zelfs maar het vermoeden bestaat dat deze in een te ruime kring bekend geworden zijn.

.

Database

- De relevante gegevens van websites van de websites van lokale Amnesty groepen (ook indien niet bij Amnesty gehost) worden -voor zover die gegevens bekend zijn- opgenomen in een database.
- Die database is niet openbaar zijn, of hooguit voor een gedeelte.
- De database dient voor het beheer van de server door het webhosting team. Een deel van de database is ook beschikbaar zijn voor de regio-coördinatoren en de monitorende leden van de InternetGroep.
- De gegevens in de database worden beheerd door het webhosting team.
- Daarbij worden uiteraard "ontvangen" gegevens gebruikt, maar ook zullen gegevens actief verzameld worden en ook van tijd tot tijd gecheckt.

Tot slot:

Veiligheid is geen zaak voor het webhosting team alleen. Vanaf de "achterkant" kan het webhosting team voor een goede basis zorgen, die in stand houden en waar nodig of mogelijk nog versterken. Om ook de "voorkant" veilig te houden is medewerking nodig van elke webmaster afzonderlijk.