Zo werkt NAAM aan een veiliger internet

Het internet biedt veel kansen voor ondernemers. Maar het is ook een omgeving waar kwaadwillenden hun slag proberen te slaan. Bij NAAM vinden we het belangrijk dat iedereen het internet veilig kan gebruiken. Als webbedrijf is het onze taak om bij te dragen aan een veiligere online wereld. Hoe we dat precies doen, leggen we graag aan je uit.

Wat we doen tegen misbruik

Helaas, het komt voor bij elke hosting en elk datacenter: misbruik. Criminelen misbruiken dan de dienstverlening van een legaal bedrijf om er illegale activiteiten op na te houden. Denk bijvoorbeeld aan phishing (het hengelen naar gevoelige gegevens), het versturen van spam, het verspreiden van schadelijke software of het uitvoeren van hacks. Bij NAAM we geen enkele vorm van misbruik van onze servers.

We hebben een abuse-adres (abuse [at] NAAM.nl). Dat houdt in dat als je overlast ervaart van een van onze klanten, je een mail naar ons kunt sturen. We nemen je klacht dan in onderzoek. Daarnaast hebben we detectiesystemen die verdachte patronen meteen signaleren. Denk bijvoorbeeld aan plotselinge pieken in mailverkeer of ongebruikelijke serveractiviteiten.

We staan geen frauduleuze websites toe

Nepwebshops of websites die zich voordoen als banken of bekende merken? Die staan we niet toe. Ze zijn een groot gevaar voor consumenten. Ontvangen we een melding dat een dergelijke site bij ons is ondergebracht, dan beoordelen we deze direct. We kijken naar screenshots, domeininformatie en serverlogs. Als er overtuigend bewijs is van fraude, halen we de website snel uit de lucht.

De klant heeft dan tijdelijk geen toegang meer tot zijn website en server. Natuurlijk is er wel ruimte voor hoor- en wederhoor. Het kan zijn dat het account gehackt is, en deze website per ongeluk te zien is. Dan stellen we de klant in de gelegenheid om het lek te dichten. Maar gaat het om criminelen, dan kunnen we zelfs de politie inschakelen.

Spam van onze servers

Spam is nog altijd een van de grootste irritaties op het internet. Ontvang je spam die verstuurd lijkt te zijn vanaf een server van Webmedia - Nijmegen? Meld het ons! Stuur het volledige bericht door, inclusief de e-mailheaders, naar onze helpdesk. In de headers staat cruciale informatie over de verzendroute en de betrokken servers.

Na ontvangst van je melding gaan we op zoek. Komt de spam echt vanuit onze infrastructuur? Of gaat het om spoofing, waarbij afzendergegevens worden vervalst? Komt het echt van onze servers, dan spreken we de verantwoordelijke klant aan en beperken we

het account. Zelf kun je spam voorkomen door je e-mailadres niet op sociale media, fora of andere websites te plaatsen. Vul je e-mailadres alleen in bij bedrijven en organisaties als dat echt nodig is. Meld je af voor ongevraagde berichten en geef er geen toestemming voor. Klik daarnaast nooit op links die je niet vertrouwt. Meer informatie over spam lees je bij de Rijksoverheid.

Samen sterk tegen illegale content

Illegale content kan van alles zijn: auteursrechtelijk beschermd materiaal, illegale handel of zaken die het daglicht niet kunnen verdragen. Wij hebben een zero-tolerance-aanpak voor illegale content. Zodra een melding binnenkomt, wordt deze direct beoordeeld door ons team. Bij zeer ernstige gevallen schakelen we de politie in. Voor bijvoorbeeld auteursrechtinbreuk geldt dat we werken met een notice-and-takedown-procedure. De klant krijgt dan de mogelijkheid het materiaal vrijwillig te verwijderen.

We investeren ook in preventieve maatregelen. Denk aan slimme scanners die geüploade bestanden scannen. Daarnaast hebben we heldere voorwaarden in onze gebruikersovereenkomsten. Zo houden we het internet voor iedereen veilig.