Introductie: Web Beveiliging

De essentie van beveiliging

In de moderne maatschappij zijn we er bijna aan gewend; vrijwel elke dag is er een datalek in het nieuws. Een organisatie die het slachtoffer is geworden van ransomware, een website die gehackt is of data die uitgelekt is naar de pers. Nog nooit is beveiliging zo essentieel geweest.

Helaas is er geen magische oplossing die je gehele online leven met dichttimmert met een druk op de knop. Beveiliging is een continu proces, een combinatie van verschillende lagen en partijen. En zelfs dan: er is geen waterdichte bescherming.

Beveiliging is het zo veilig mogelijk maken, het opwerpen van een zo hoog mogelijke barriere. Dat vereist een samenwerking tussen alle partijen. Om een voorbeeld te geven: als hoster kunnen wij het nog zo dichttimmeren, maar als de klant overal hetzelfde wachtwoord gebruikt, of een combinatie admin/admin gebruikt is dat irrelevant; je zet daarmee immers de voordeur wagenwijd open.

Deze whitepaper geeft een introductie aan hoe je als webbouwer veilig(er) te werk kunt gaan en een veilige start kunt maken. Vanaf 2024 gaan wij - Routehost - masterclasses aanbieden die in veel meer detail over alle aspecten heen gaan. Mocht je hierin interesse hebben, laat het ons zeker weten.

En als je nog vragen hebt, twijfel niet om contact op te nemen. Onze experts zitten voor je klaar op support@routehost.nl.

Enjoy & be safe!

Het Routehost team

Wat Routehost doet

Het fundament van de beveiliging van jouw websites ligt bij de webhoster. In dit geval bij ons, als Routehost zijnde. Met een hele sterke focus op veiligheid zijn wij bewuster en innovatiever dan de meeste concurrenten. Om een idee te geven van wat wij doen:

- **01. Fysieke toegang:** onze servers zijn geplaatst in veilige datacenters. Alleen een deel van de Routehost engineers heeft toegang; zij moeten zichzelf aanmelden bij de beveiliging welke er 24/7 is, door een toegangspoort met biometrische bveiliging, vervolgens naar de suite welke een toegangspas vereist en dan het rack ontgrendelen met een sleutel. Dit hele proces wordt tevens nauwlettend gemonitord met 24/7 camerabewaking.
- **02. Firewalling:** onze infrastructuur - dus de servers en het netwerk - is voorzien van meedere firewalls. Dit is de eerste laag in de beveiliging. Net als de beveiliging op een luchthaven kijkt de firewall of bezoekers op de gastenlijst staat en fouilleert de bezoekers vervolgens of ze geen wapens dragen.
- **03. Webserver:** op de shared hosting maken wij gebruik van een combinatie van Apache httpd en nginx (als reverse proxy). Niet alleen kunnen we hiermee extra snelheid bieden (door middel van caching en het sneller serveren van static content), maar ook de TLS laag veilig implementeren. TLS zorgt ervoor dat de verbinding tussen de server en bezoeker versleuteld is. Wij maken hierbij gebruik van de meest hoge graad van versleuteling.
- **04. Isolatie:** alle websites draaien in een eigen, hermetisch afgesloten container. Hierdoor is er geen overlast of hinder als een andere klant zich misdraagt of een gehackte website heeft. Wel zo veilig!
- **05. Server hardening:** de servers waarop het shared hostingplatform draait zijn voorzien van verregaande hardening; van de kernel tot aan de configuratie van de daemons/services.
- **06. Updates:** we voeren wekelijks updates door voor onze servers. En als het nodig is - omdat de update bijvoorbeeld een kwetsbaarheid dicht, dan doen we dit binnen vier uur nadat de update beschikbaar is gesteld.

Backups

Wij maken elke nacht een volledige backup van alle omgevingen; de websites (bestanden, databases), e-mail, instellingen en overige data. Die bewaren wij dertig dagen. Backups worden op een manier gemaakt waarbij de server zelf geen toegang hiertoe heeft; dus eventuele malware kan deze ook niet aantasten of verwijderen. Ook worden de backups in meerdere locaties (datacenters) opgeslagen.

Beveiligde verbinding

Om te zorgen dat de verbinding tussen de bezoeker en de website/email beveiligt is, maken wij gebruik van TLS - dit wordt vaak nog SSL genoemd, wat de oude vorm is. Om het heel simpel te zeggen: dat is het "slotje in beeld". Deze techniek zorgt ervoor dat de verbinding tussen de bezoeker en de website of mailserver versleuteld is - dus niet af te tappen door kwaadwillenden.

De achterliggende techniek werkt door middel van PKI certificaten. Gedurende een lange tijd hebben hier kosten aan gezeten; de organisaties die de certificaten uitgeven (CA's, Certificate Authorities) vroegen hier immers geld voor; van enkele tientjes per jaar tot honderden euro's.

Dat is inmiddels niet meer het geval. Er zijn verschillende partijen die gratis certificaten aanbieden, welke net zo veilig zijn als de commerciele versies. Routehost maakt gebruik van Let's Encrypt en ZeroSSL om te zorgen dat jouw website en mail standaard al is voorzien van een TLS verbinding. Dat gaat automatisch, je hoeft daar zelf niets voor te doen. Dat is nog eens handig!

Er zijn een paar uitzonderingen, waarin zo'n Lets Encrypt of ZeroSSL niet volstaat:

- Bij communicatie met de overheid - dan is een PKIoverheid certificaat nodig. Dit is bijvoorbeeld het geval voor een accountant die belastingaangifte wil indienen bij de belastingdienst. Of een zorgaanbieder die moet communiceren met partijen als Vecozo en UZi om verzekeringsgegevens op te halen.
- Bij bepaalde zeer gevoelige en kritische markten. Denk bijvoorbeeld aan een bank. Dan is een EV (Extended Validation) certificaat nodig; welke niet alleen het eigendom van het domein checkt, maar ook het hele bedrijf.

Routehost kan de aanvraag van die certificaten ook faciliteren. Maar indien je niet onder een van die twee uitzonderingen valt, hoef je niets te doen en wordt jouw pakket automatisch voorzien van een certificaat.

De rol van webbouwers

Als webbouwer ben je een stukje kwetsbaarder; je hebt immers toegang tot meerdere websites die je bouwt en onderhoud. Hierdoor ben je extra gebaat bij een goede beveiliging - niet alleen van de websites, maar ook van jouw eigen computer of laptop.

- **Updaten:** niet het meest leuke klusje - maar updates zijn een enorm belangrijke beveiliging tegen indringers. Zorg ervoor dat je elke week de updates van je computer en/of laptop doorvoert. En ook: maak geen gebruik van verouderde software. Als je bijvoorbeeld een Mac uit 2012 hebt, kun je niet upgraden naar de meest recente versie van macOS; waardoor je een gigantisch risico loopt.
- **Antimalware en firewall:** maak gebruik van oplossing tegen malware en een firewall. Ongeacht of je Windows of macOS gebruikt, er zijn virussen, ransomware en andere narigheid voor elk platform. Indien je macOS gebruikt: open de systeemvoorkeuren en check of de firewall staat ingeschakeld. Het is hier aanzienlijk beter om de 'stealth modus' in te schakelen, welke je onder de knop Opties kunt vinden.
- **Wachtwoorden:** gebruik overal sterke en unieke wachtwoorden. Die hoef je gelukkig niet zelf te onthouden - daarvoor is een wachtwoord manager een hele fijne toevoeging. Aanraders zijn KeePassXC, Bitwarden en 1Password.
- **Links in e-mail:** wees heel voorzichtig met het aanklikken van links in e-mailberichten. Het beste is om helemaal geen links aan te klikken; stel dat je een mail krijgt dat er een bericht van je bank, de overheid of dokter voor je klaar staat, gebruik dan niet de link in de e-mail, maar ga zelf naar de website toe, login en check het bericht.
- **Software-bronnen:** gebruik alleen de Windows of Apple store om software te downloaden - en als het echt niet anders kan, download de software dan direct van de ontwikkelaar in plaats van een willekeurige download site (hoe betrouwbaar deze er dan ook uitziet). Gebruik nooit illegale software, cracks of keygens, de kans is enorm groot dat hier malware aan zit. Dit geldt overigens ook voor web scripts (zoals WordPress plugins, thema's etc). Je zal niet de eerste zijn die de marge wilt vergroten en daardoor met een gehackte site te maken krijgt.
- **Wees waakzaam:** de zwakste schakel in de beveiliging is - helaas - de mens. Wees daarom altijd waakzaam; bij eventuele vragen: schiet ons een mail op support. Liever een vraag te veel dan te weinig. En schaam je niet; een ongeluk zit in een klein hoekje en kan ons allemaal overkomen. Hoe eerder we een melding krijgen, hoe meer we de impact kunnen inperken.

Wat je zelf kunt doen voor WordPress

- Maak een beheerdersaccount met een unieke username; gebruik geen 'admin' als username. Mocht je dit al wel gedaan hebben, maak dan een nieuwe aan met beheerdersrechten, log daarop in en verwijder de voormalige admin gebruiker. Wijs tijdens het verwijderen de bestaande content toe aan de nieuwe beheerder.

- Gebruik een beveiligingsplugin; een sterke aanrader is WordFence. Zelfs de gratis versie biedt een betere beveiliging dan de meeste andere oplossingen hiervoor. Dit is ook een hele goede vervanger van iThemes Security.

- Gebruik zo min mogelijk plugins - en check of de plugins die je gebruikt nog actief onderhouden worden.

- Installeer regelmatig - minimaal wekelijks - de updates van WordPress, de plugins en thema's.

- Schakel 2FA / MFA in voor de beheerders.

- Gebruik een centrale beheertool zoals managewp.com voor eenvoudiger beheer, onderhoud en updates.

Routehost