Bescherm uw domein met SPF tegen phishingmails

Met een paar stappen kunnen bedrijven (en particulieren) hun eigen e-maildomein een stuk veiliger maken. De kans op misbruik kan zo flink worden teruggedrongen.

Veel criminaliteit op internet begint met het versturen van een e-mail. Vaak doen de afzenders zich voor als een bestaand bedrijf. Natuurlijk wilt u het deze lieden zo lastig mogelijk maken en voorkomen dat de naam van uw bedrijf wordt misbruikt.

Nu is het voor kwaadwillenden vaak relatief eenvoudig om e-mails te versturen namens een ander. Verschillende websites bieden een dienst aan waarmee (als grap) een e-mail gestuurd kan worden namens Michael Jackson, de koning of een willekeurig ander bekend persoon. Maar waar het hier gaat om een enkel mailtje, kunnen oplichters dit ook op grote schaal doen.

Als ondernemer wilt u voorkomen dat anderen onder uw naam e-mails kunnen versturen. Er zijn drie beveiligingstechnieken die u hierbij van dienst kunnen zijn: Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) en Domain-based Message Authentication, Reporting and Conformance (DMARC). Met name SPF is relatief eenvoudig te installeren en ondervangt voor een aanzienlijk deel het risico.

Wat is SPF?
Met SPF regelt u welke servers namens uw domein (alles achter @ in een e-mailadres) berichten mogen verzenden. Als vervolgens een e-mail wordt ontvangen vanuit uw domein, dan controleert de ontvangende server of het een legitiem bericht is. Komt het van een server die niet is goedgekeurd, dan wordt de mail tegengehouden of gemarkeerd als onveilig.

Stappen om SPF te realiseren
SPF kunt u bij verschillende websites genereren (bijvoorbeeld via https://spfrecord.io/). U vult hier in wat uw domeinnaam is en geeft aan welke servers e-mail namens dit domein mogen verzenden. Vervolgens dient u het SPF-record in de DNS instellingen van uw website op te nemen, als tekst (TXT) veld.

Let op! Is uw eigen technische kennis ontoereikend of twijfelt u over de juiste instellingen? Vraag dan uw ICT-leverancier SPF in te stellen. Dit is belangrijk, want het verkeerd instellen van SPF kan ervoor zorgen dat u geen e-mail meer kunt versturen.

Een SPF-record ziet er als volgt uit:
"v=spf1 mx a ip4:127.0.0.1 include:example.com ~all"

Dit record bestaat uit drie verschillende onderdelen, gescheiden door spaties. Het eerste deel (v=spf1) geeft aan dat we met een SPF record te maken hebben. Het middelste deel bestaat uit alle servers (ip-adressen) die e-mail mogen sturen namens uw domein. Het laatste deel geeft aan wat ontvangers moeten doen als ze een e-mail ontvangen die niet door een van de toegestane servers verstuurd is. We gaan iets dieper in op de middelste en laatste delen.

Allereerst het middelste deel. Zoals gezegd geven we hier aan welke servers e-mails mogen sturen. In ons voorbeeld is de eerste server die mag mailen "mx". Dat betekent dat de mailservers die voor uw domein zijn ingesteld, e-mails mogen sturen. Deze mailservers worden in DNS aangegeven met een "MX"-record. Daarachter staat "a", wat betekent dat de webserver e-mails mag versturen, dat wil zeggen, het "A"-record in uw DNS instellingen. Vervolgens mag het ip-adres 127.0.0.1 e-mails versturen, en als laatste staat er een "include:example.com". Dit betekent dat alle servers die e-mails mogen versturen namens example.com, dit ook voor uw domein mogen doen. Dat is erg handig wanneer u verschillende domeinen heeft. U stelt dan bij een van de domeinen (bijvoorbeeld fraudehelpdesk.nl) een SPF record in, en bij alle andere domeinen zet u "include:fraudehelpdesk.nl" neer. Hierdoor hoeft u alleen nog voor uw hoofddomein een SPF record aan te passen.

Als laatste bevat een SPF-record een code om te bepalen wat er dient te gebeuren met foute e-mails. In ons voorbeeld staat er "~all". Het eerste teken mag een min-teken zijn (-, afwijzen van de e-mail), een tilde (~, markeren van de e-mail), een plus-teken (+, negeren / maakt niet uit) of een vraagteken (?, neutraal / geen mening). Het teken moet altijd worden gevolgd door het woord 'all'. Als u als teken een vraagteken of een plus-teken kiest, dan heeft het SPF-record geen effect op de verzonden e-mails. Dit kan handig zijn om te testen, maar beschermt u dus niet tegen fraudeurs.

DKIM en DMARC

Naast SPF zijn DKIM en DMARC ook hulpmiddelen waarmee het lastiger wordt voor criminelen om spam en phishingmails namens uw organisatie te versturen. DKIM en DMARC werken aanvullend op SPF en zijn geen vervangers. Wel zijn ze minder eenvoudig te installeren dan SPF.

DKIM is het digitaal ondertekenen van e-mail. Door deze digitale handtekening onder een e-mail kan de ontvanger controleren dat het een legitieme e-mail is. Om DKIM te activeren, dient u twee acties te ondernemen: (1) de e-mail server die u gebruikt dient alle e-mails digitaal te ondertekenen; en (2) u dient een TXT DKIM-record toe te voegen aan uw domein. Hierin geeft u aan hoe de correcte handtekening eruit ziet. Wanneer u DKIM wilt gebruiken, raden wij u aan om contact op te nemen met uw ICT- leverancier.

DMARC is een soort beleid voor een domein waarin staat wat er moet gebeuren wanneer DKIM en SPF aangeven dat een e-mail niet legitiem is. U kunt bijvoorbeeld instellen dat een e-mail dan naar de spam map van de ontvanger moet gaan. Of dat een foute e-mail compleet verwijderd moet worden. Daarnaast kunt u instellen dat u dagelijks rapportages ontvangt met informatie over alle ontvangen e-mails vanuit uw domein. Dit kan erg handig zijn om inzicht te geven in de e-mailstromen