E-MAILBEVEILIGING

Met onze e-mailbeveiliging gaan wij een stapje verder dan andere hostingproviders:

- Wij richten alle beveiligingstechnieken voor jou in.
- Onze beveiliging voldoet aan de huidige e-mailbeveiligingsnormen.

Wij beveiligen jouw e-mailverkeer tegen:

Spam Massaal verstuurde ongewenste e-mails.

Domeinnaammisbruik Hackers gebruiken jouw domeinnaam om e-mails te verzenden (spoofing) of om de ontvanger naar een valse website te lokken om geld of gegevens te stelen (phishing).

Aftappen Hackers onderscheppen informatie in het e-mailverkeer tussen jou en de ontvanger zonder dat jullie dit doorhebben. Dit kan gebeuren bij inkomende- en uitgaande mails.

BEVEILIGING TEGEN SPAM

Wij bieden bij onze hosting een standaard, gratis spamfilter. Deze applicatie filtert e-mails voordat ze jouw inbox bereiken op basis van een lijst van al bekende veelvoorkomende spam. Het standaard spamfilter moet je zelf nog instellen. Wil je hier hulp bij? Mail naar support@brisp.nl of bel +31 (0)50 2011 460.

Als je jouw inbox nog beter wil beveiligen is de betaalde spamfilter een goede optie. De betaalde spamfilter geeft aan iedere inkomende en uitgaande e-mail een spamscore met behulp van zelflerende software. Is de spamscore van een e-mail te hoog? Dan houdt de spamfilter de e-mail tegen.

MEER WETEN? MAIL ONS VIA INFO@BRISP.NL OF BEL NAAR +31 (0)50 535 1752.

BEVEILIGING TEGEN DOMEINNAAMMISBRUIK EN HET AFTAPPEN VAN E-MAILS

SPF verhindert hackers zodat ze geen e-mails kunnen sturen vanuit jouw domeinnaam. Alle e-mails met een onbekende verzender worden door onze strenge instellingen niet afgeleverd. Wil jij via een niet bekende afzender een e-mail sturen vanuit jouw domeinnaam? Geef dit aan ons door en wij controleren of de afzender bekend is in het SPF.

DKIM zorgt ervoor dat jij een unieke, digitale handtekening hebt voor jouw domeinnaam. Hiermee kan je bewijzen dat de e-mails die jij verzendt ook echt van jou zijn.

DMARC controleert de resultaten van SPF en DKIM. Als de identiteit van de afzender correct is wordt de e-mail doorgelaten. Klopt er iets niet? Dan wordt de e-mail standaard door ons geblokkeerd en niet afgeleverd.

DNSSEC In het DNS staat naar welk IP-adres jouw domeinnaam en e-mail verwijzen. Dit is vergelijkbaar met een telefoonboek, waarbij een naam naar een bepaald telefoonnummer verwijst. DNSSEC zorgt voor een slot tussen jouw e-mailserver en IP-adressen in jouw DNS. Dit verhindert hackers zodat ze niet e-mails kunnen onderscheppen die je verstuurt of ontvangt.

SSL/TLS voorziet het mailverkeer van versleuteling. Dit verhindert hackers die de inhoud van jouw e-mails willen onderscheppen.

DANE controleert de identiteit van de ontvanger van jouw e-mail. Dit verhindert hackers als ze zich voor willen doen als de ontvanger. Ze kunnen dan niet jouw e-mails onderscheppen. Daarnaast dwingt DANE de versleuteling van SSL/TLS af.

16-11-2022 | BRISP | Helperpark 272-4 | 9723 ZA Groningen | Nederland | sales@brisp.nl | +31 (0)50 2011 455 | Prijswijzigingen en typefouten voorbehouden.