

Diverse openbare databases veronderstellen dat het IP-adres [IP-nummer invoegen] mogelijk een zogeheten open relay mail server of een open proxy server is.

Wij nemen aan dat u een server heeft die dit IP-adres gebruikt. Deze e-mail bevat belangrijke informatie die effect kan hebben op de online aanwezigheid van uw organisatie. Indien u niet de geregistreerde eigenaar bent van dit IP-adres, wilt u dan zo vriendelijk zijn dit bericht door te sturen naar de juiste contactpersoon.

Wij zenden deze e-mail als onderdeel van het project "Operation Secure Your Server," een gezamenlijk project van de United States Federal Trade Commission en andere overheidsorganisaties wereldwijd, die betrokken zijn bij de problemen die voortvloeien uit de groei van ongevraagde commerciële e-mail (spam).

Wij willen u uitleggen hoe u uw servers kunt beveiligen en voorkomen dat deze een onbedoelde bron van spam worden.

Als eerste maatregel stellen wij u voor dat u uw open relay of open proxy server afsluit. Open relays en open proxies zijn servers die toestaan dat iedere computer in de wereld e-mail doorstuurt of verzendt naar andere Internet mailadressen. Open relays en open proxies worden vaak misbruikt door mensen die het Internet overspoelen met spam. Dit misbruik veroorzaakt wereldwijd problemen voor abonnees, voor toezichthouders en voor uw organisatie.

Ontvangers van spam veronderstellen bijvoorbeeld dat de spam van uw systeem afkomstig is en onbekende derde partijen kunnen uw servers en internetaansluiting misbruiken. Hierdoor kan uw netwerk overbelast raken met spamverkeer. Als gevolg hiervan kunnen uw administratieve kosten toenemen. Ook kan uw Internet Service Provider ertoe overgaan om uw Internetaansluiting af te sluiten. Beveiliging van uw server helpt u om uw systeem te beveiligen tegen misbruik.

Wij bieden u aanvullende informatie over open relays, open proxies en over hoe u uw organisatie kunt beschermen tegen de gevaren van onbeveiligde servers, inclusief stap-voor-stap instructies over hoe deze servers af zijn te sluiten.

Klik op [www.ftc.gov/secureyourserver](http://www.ftc.gov/secureyourserver) om de webpagina over dit onderwerp te bekijken, inclusief een lijst met aan dit project deelnemende organisaties. Voor directe toegang tot de instructies voor het afsluiten van uw open relay of open proxy, klik op [www.ftc.gov/bcp/online/pubs/buspubs/secureyourserver.htm](http://www.ftc.gov/bcp/online/pubs/buspubs/secureyourserver.htm).

Indien u vragen heeft over de instructies of deze brief, schrijft u dan alstublieft naar [secureyourserver@ftc.gov](mailto:secureyourserver@ftc.gov).