**Artikel 1** | Implementeer veilige e-mailstandaarden en voorkom cyberaanvallen

*E-mail is een van de meest gebruikte communicatiemiddelen, vooral binnen ondernemingen en organisaties. Naar verwachting groeit het aantal e-mailgebruikers wereldwijd verder tot 4,6 miljard gebruikers in 2025 (*[*Statista, 2022*](https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/)*). E-mail is ontwikkeld in de beginjaren van het internet en het concept is gebaseerd op de traditionele brievenpost. Daardoor kent e-mail verschillende kwetsbaarheden. Het is voor cybercriminelen de belangrijkste manier om toegang te krijgen tot systemen en gegevens. Zij gebruiken vervalste mailadressen in combinatie met phishing, malware en spoofing om persoonsgegevens of andere informatie te achterhalen en geld afhandig te maken van personen of bedrijven. Om de gevolgen van online fraude en kwaadaardige software te voorkomen, is het belangrijk dat bedrijven zorgvuldig omgaan met e-mail en hun mailverkeer goed beveiligen. Dat kan door veilige en moderne e-mailstandaarden te implementeren.*

**Phishing en social engineering**

Uit een onderzoek van CISCO blijkt dat 90% van alle online inbreuken plaatsvindt via phishing (CISCO-rapport Cybersecurity Threat Trends, 2021). De schade door phishing naar beveiligingscodes van bankrekeningen liep in 2022 op tot € 3,6 miljoen. Phishing is een vorm van social engineering, waarbij oplichters zich voordoen als een betrouwbare bron. Zij versturen valse e-mails die afkomstig lijken van officiële instanties, zoals een bank of zorgverzekeraar. Als de ontvanger van zo’n mail doorklikt, komt deze terecht op een website die lijkt op die van een officiële organisatie. Via bijvoorbeeld een inlogscherm krijgt de ontvanger de vraag om persoonlijke gegevens of een bankrekening in te vullen. Daarnaast kan het openen van phishingmails ervoor zorgen dat er malware op de computer geïnstalleerd wordt. Denk aan ransomware die de gegevens op een computer versleutelt, waardoor de gebruiker hier niet meer bij kan. Om weer toegang te krijgen tot de versleutelde gegevens eisen de cybercriminelen losgeld, vaak in de vorm van cryptogeld.

**Ransomware-aanval op de Universiteit van Maastricht**

Dit overkwam de Universiteit van Maastricht. In 2019 werd de universiteit slachtoffer van een grote ransomware-aanval. Medewerkers ontvingen 2 phishingmails met daarin een link met een virus. Nadat een medewerker de mail opende, wisten de internetcriminelen bestanden van de universiteit te versleutelen. Uiteindelijk betaalde de universiteit 30 bitcoins aan de hackers, om weer toegang te krijgen tot de bestanden op 267 servers van het Windows-domein. Het bedrag kwam neer op zo’n € 200.000 euro. De Universiteit van Maastricht was zeker niet het enige slachtoffer van hackers of online fraude. Ook organisaties als Artis, MediaMarkt, RTL Nederland en Veiligheidsregio Noord- en Oost-Gelderland hadden te maken met cyberaanvallen.

**Moderne en veilige e-mailstandaarden**

Zo’n 96% van de Nederlandse bedrijven heeft het e-maildomein onvoldoende beveiligd (ABN Amro en MWM2, 2022). Dat is zorgelijk, want zoals je las komen cyberaanvallen regelmatig voor. Om e-mail te beveiligen zijn er diverse standaarden beschikbaar. Zo gaan e-mailstandaarden als DANE, SPF, DKIM en DMARC phishing, spam en malware tegen. Dit doen ze door de afzender, het mailsysteem en de inhoud van een e-mail te beveiligen. Deze standaarden worden vaak gezamenlijk ingezet, omdat ze elkaar kunnen versterken. DMARC versterkt de werking van SPF en DKIM en DANE wordt alleen toegepast in combinatie met DNSSEC.

**Massale implementatie**

Het massaal toepassen van veilige e-mailstandaarden is belangrijk. Als ondernemingen en bedrijven veilige e-mailstandaarden op grote schaal implementeren, ontstaat er een uniforme aanpak van e-mailbeveiliging. Zo kunnen bedrijven en systemen beter onderling samenwerken en gemakkelijker veilig online communiceren. Daarnaast zorgt massale adoptie van de standaarden ervoor dat het voor cybercriminelen moeilijker is om kwetsbaarheden te vinden. Massale adoptie betekent dat veilige e-mailstandaarden op alle domeinnamen en alle verzendende en ontvangende mailservers worden geïmplementeerd. Wil je direct starten met de implementatie van veilige e-mailstandaarden? Bekijk dan ons artikel over het bestrijden van phishing, spoofing en malware met veilige e-mailstandaarden.

*Ga naar* [*sidn.nl/moderne-internetstandaarden/e-mailbeveiliging*](https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging) *voor meer informatie over veilige e-mailstandaarden als STARTTLS en DANE.*