Cyber
Weerbaarheidscentrum
Greenport

E-mail: veilig gebruik

Tips voor het gebruik van e-mail

Er liggen veel risico's op de loer bij het gebruik van e-mail. Hier zijn enkele basis zaken die je als ondernemer in het achterhoofd dient te houden:

- **Leid je medewerkers op**
  Zorg ervoor dat medewerkers binnen jouw organisatie weten wat, los van de positieve effecten, de gevaren zijn van e-mail. Bied trainingen aan die hen bekend maken met de risico's die zich voordoen via de e-mail.

- **Open geen onbekende bijlages**
  Open nooit onbekende bijlages in e-mails. Dit geldt zelfs voor bestanden die afkomstig zijn van een bekende en er wellicht ongevaarlijk uit zien. Ook afbeeldingen of pdf-bestanden kunnen kwaadaardige code bevatten.

- **Check wie de afzender is**
  Vertrouw niet blind op de afzender van de e-mail. Bekijk goed van wie de e-mail afkomstig is. Reageer nooit op e-mails waarvan jij niet zeker bent van de afzender of het emailadres.

- **Klik niet zomaar op links**
  Het goed inspecteren van een verdachte link kan geen kwaad. Argeloos klikken (zelfs al klik je maar 1 keer) kan jou slachtoffer maken van een phishing aanval.

- **Geloof niet alles**
  Blijf kritisch en geloof niet alles wat je leest. Een mooie financiële deal of samenwerking met een grote partij klinkt mooi en aanlokkelijk. Maar is de e-mail daadwerkelijk afkomstig van de persoon die hij/zij zegt te zijn?

- **Je mailbox is geen verzamelplaats**
  Sla belangrijke gegevens niet alleen op in de e-mail. Gebruik jouw mailbox niet als verzamelplaats.

- **Koppel geen persoonlijke diensten**
  Koppel geen persoonlijke services/diensten van derde partijen aan jouw zakelijke e-mailadres. Denk hierbij bijvoorbeeld aan het aanmaken van een Facebook account op jouw zakelijke e-mailadres.

E-mail beveiligingsstandaarden

E-mail is nog steeds de meest gebruikte vorm van communicatie tussen bedrijven, partners en klanten. Vaak is e-mail noodzakelijk voor het functioneren van bepaalde bedrijfsprocessen zoals de facturatie of het versturen van een orderbevestiging bij een bestelling. Het is dus van belang dat een ontvanger een e-mail daadwerkelijk ontvangt en er van uit kan gaan dat deze ook echt afkomstig is van jouw organisatie. Om dit te kunnen waarborgen maken we gebruik van beveiligingstandaarden voor e-mails.

Waarom zijn er e-mail beveiligingsstandaarden?

E-mail is een veel gebruikte vorm van communicatie waar veel organisaties afhankelijk van zijn. De meeste organisaties gebruiken een eigen e-maildomein zodat e-mailadressen herkenbaar en herleidbaar overkomen.

E-mail is echter niet de meest veilige en betrouwbare vorm van communicatie. Zonder aanvullende inrichting binnen jouw e-mailomgeving, kun je tegen de volgende risico's aanlopen:

- Het is vrij eenvoudig het e-maildomein van jouw organisatie te 'spoofen'. Dit houdt in dat iemand e-mails kan versturen met een e-mailadres van jouw organisatie als afzender. Phishing-aanvallen hebben op deze manier een grotere kans van slagen omdat de ontvanger het e-mailadres van de afzender (ten onrechte) vertrouwt. Zowel medewerkers binnen je eigen organisatie als daarbuiten kunnen hier slachtoffer van worden;
- Het ontbreken of verkeerd toepassen van e-mail beveiliggingsstandaarden kan ervoor zorgen dat e-mails die jouw organisatie verstuurt, niet worden vertrouwd door de ontvangende e-mailomgeving. Afhankelijk van hoe streng de ontvangende mailserver is ingesteld, komen de e-mails mogelijk niet aan bij de ontvanger of worden ze aangeduid als 'spam';
- De communicatie tussen de verzendende mailserver en ontvangende mailserver gebeurt onversleuteld waardoor e-mailberichten inzichtelijk zijn of kunnen worden aangepast voordat deze de ontvanger bereiken.

E-mailbeveiliging

Als er gesproken wordt over e-mailbeveiliging wordt vaak aandacht besteed aan het beschermen tegen phishing, spam of malware aan de ontvangende kant. Dit is uiteraard belangrijk, maar e-mailbeveiliging gaat verder dan het hebben van een goed spamfilter en het trainen van medewerkers om "foute" e-mails te herkennen. De risico's die hierboven beschreven worden hebben invloed op de beschikbaarheid, integriteit en vertrouwelijkheid van e-mails die jouw organisatie verzendt. Door maatregelen te nemen tegen deze risico's, draag je ook bij aan het veiliger maken van e-mail aan de kant van de ontvanger.

E-mail authenticatie

De volgende 3 beveiligingsstandaarden worden gebruikt voor e-mail authenticatie. Dit maakt het mogelijk voor de ontvangende partij om te verifiëren of e-mail van een bepaald maildomein afkomstig is van iemand die daartoe bevoegd is. Dit helpt spoofing voorkomen en helpt ook bij de afweging of een e-mailbericht spam is.

1. Sender Policy Framework (SPF)
Sender Policy Framework (SPF) is een standaard waarmee je kunt aangeven welke IP-adressen er namens het maildomein van jouw organisatie e-mailberichten mogen versturen ((en welke niet). Deze informatie wordt opgeslagen in het zogenoemde "SPF-Record" van het maildomein. Dit record wordt via **DNS** uitgelezen door de ontvangende mailserver. IP-adressen die je hierin kwijt wilt, zijn adressen van servers die de e-mails van jou en jouw medewerkers uitsturen, maar ook de server die bijvoorbeeld de facturen of een bedrijfsnieuwsbrief uitstuurt. Het hebben van een SPF-Record verhoogt het vertrouwen bij de ontvangende mailserver in de afweging of jouw bericht spam is.

2. DomainKeys Identified Mail (DKIM)
DomainKeys Identified Mail (DKIM) zorgt er voor dat er een 'vingerafdruk' wordt toegevoegd aan een e-mail. De ontvangende mailserver gebruikt deze vingerafdruk om na te gaan of een e-mail afkomstig is van een vertrouwde mailserver en of er tijdens het transport van de e-mail iets veranderd is aan het bericht. De genoemde vingerafdruk is gebaseerd op een certificaat waarvan een ontvangende mailserver de publieke sleutel kan ophalen uit een DNS Record van het maildomein. Ook deze techniek helpt de ontvangende mailserver in de afweging of een bericht als spam wordt aangemerkt.

3. Domain-based Message Authentication, Reporting & Conformance (DMARC)
De beveiligingsstandaarden SPF en DKIM kunnen afzonderlijk van elkaar worden geconfigureerd en bieden op zichzelf al een verbetering op het gebied van de e-mail veiligheid. Domain-based Massage Authentication, Reporting & Conformance (DMARC) is ontwikkeld om door middel van een 'policy' een link te leggen tussen SPF en DKIM. Het geeft aan hoe een ontvangende mailserver dient om te gaan met de resultaten van deze 2 standaarden. Daarnaast kun je met de rapportage mogelijkheid van DMARC een beeld te krijgen of er misbruik wordt geconstateerd door een ontvangende mailserver. Mocht er zo'n rapportage zijn van mogelijk misbruik, dan kan dit ook liggen aan een foutieve configuratie van DKIM of SPF waardoor valide e-mails mogelijk niet aankomen. Ook een DMARC policy wordt opgeslagen in een DNS record van het maildomein.

Versleutelen (STARTTLS)

Het is belangrijk om te beseffen dat wanneer je een e-mail verstuurt, er geen garantie is dat het transport **versleuteld** is. Zonder versleuteling kan een e-mail naar bijvoorbeeld een klant inzichtelijk zijn voor anderen. Dit is in het geval van een nieuwsbrief waarschijnlijk geen groot probleem, maar de kans is natuurlijk ook aanwezig dat een e-mail gevoelige (persoons)gegevens bevat.

Bij dit beveiligingsprobleem hebben we te maken met het SMTP-protocol. Dit protocol wordt gebruikt om e-mails te verzenden en te ontvangen tussen de mailservers. De mogelijkheid om dit verkeer te versleutelen, gebeurt via STARTTLS. Dit staat bekend als “opportunistische versleuteling”; je kunt er gebruik van maken, maar het is niet noodzakelijk. Daarnaast zorgt een gebrek aan juiste inrichting van STARTTLS ervoor dat validatiemogelijkheden veelal ontbreken. Daardoor is het voor hackers relatief eenvoudig om een versleutelde verbinding tussen mailservers te voorkomen of een versleutelde verbinding met een verkeerde server op te laten zetten. Kortom, STARTTLS kent helaas tekortkomingen waarbij het belangrijk is om stil te staan bij een aantal punten:

- **Afspraken**
  Ondanks dat er technische oplossingen zijn die de tekortkomingen van STARTTLS tot zekere hoogte kunnen omzeilen, zijn deze oplossingen nog niet veel in gebruik. Daarnaast dek je hiermee niet het volledige transport van e-mail af. Zelfs als je 100% zeker weet dat het verkeer tussen mailservers via STARTTLS verloopt met de juiste mailservers, is het e-mailbericht alsnog onversleuteld terug te vinden op de mailservers waar het bericht langs gaat. Omdat versleutelde transport dus lastig te garanderen is, helpt het om binnen je organisatie afspraken te maken wat je wel of niet verstuurt via e-mail. Denk hier bijvoorbeeld aan BSN-nummers of wachtwoorden.

- **DNS-based Authentication of Named Entities (DANE)**
  Voor hackers is het mogelijk om versleutelde verbinding te voorkomen of een versleutelde verbinding te laten opzetten met een andere (verkeerde) server. Door middel van DNS-based Authentication of Named Entities (DANE) kunnen deze problemen worden verholpen door in de DNS van het maildomein via een zo genaamd “TLSA Record” aan te geven welke servers er e-mails mogen ontvangen en dat dit versleuteld dient te gebeuren. Je bent bij deze techniek echter afhankelijk van de ontvangende partij die dit inricht voor zijn maildomein.

- **STARTLS forceren**
  De meeste mailservers hebben de mogelijkheid om STARTTLS te forceren. Het risico is echter dat daardoor mails niet aankomen wanneer STARTTLS niet ondersteund wordt door de ontvanger. In de praktijk wordt dit daarom vaak alleen ingericht tussen partijen die van elkaar weten dat STARTTLS mogelijk is.

Draag bij aan een veiliger e-mail klimaat

Door als organisatie aandacht te besteden aan het veilig inrichten van je e-mail omgeving aan zowel de verzendende als ontvangende kant, draag je automatisch bij aan een veiliger e-mail klimaat. Zie voor meer informatie ook de factsheets van het NCSC over STARTSSL en DANE en SPF, DKIM en DMARC.

DNSSEC

De genoemde e-mail beveiligingsstandaarden leunen veel op informatie die staat opgeslagen in de DNS. Deze informatie halen mailservers op om bijvoorbeeld binnen het SPF-record na te gaan of een mailtje van een vertrouwde server afkomstig is. Om ervoor te zorgen dat dit soort informatie binnen een DNS-verzoek niet kan worden gemanipuleerd, is het belangrijk dat de DNS Server die het e-maildomein van jouw organisatie bevat, DNSSEC ondersteunt. Op deze manier voorkom je dat de e-mail beveiligingsstandaarden alsnog omzeild kunnen worden. De e-mail test van internet.nl laat zien of DNSSEC in gebruik is.

Cyber
Weerbaarheidscentrum
Greenport

Geavanceerde informatie over e-mail

Er zijn meerdere manieren om je e-mail in te richten. Je kunt de hosting van je e-mail zelf verzorgen (on-premise) of uitbesteden aan een externe hostingpartij (cloud). Welke optie je kiest, is volledig afhankelijk van de wensen, eisen en/of de aanwezigheid van een (systeem)beheerder binnen jouw organisatie.

Voor- en nadelen van on-premise en cloud

In het geval van lokale hosting (on-premise) ben je zelf verantwoordelijk voor de aanschaf van hard- en software, hosting, beheer, onderhoud en het treffen van beveiligingsmaatregelen. Uiteraard heb je met e-mail in eigen beheer meer flexibiliteit. Zo hoef je niet te betalen voor extra opslagruimte en kun je gemakkelijk ongelimiteerd veel e-mailaccounts toevoegen.

Het nadeel van e-mailhosting in eigen beheer is dat het onderhouden, up-to-date houden, bewaken en spam-vrij houden van een dergelijk systeem veel tijd in beslag kan nemen van een systeembeheerder. Onder de streep kan het dan toch nog duurder uitvallen dan een oplossing in de cloud. Wanneer je de hosting van de e-mail bij een derde partij belegd heb je geen initiële investeringskosten voor hard- en software, is geen beheerder nodig en wordt het systeem up-to-date gehouden door de provider. Ook beveiligingsmaatregelen worden door de clouddienstverlener getroffen en wordt zo dus een groot gedeelte van de beveiligingsrisico's uitbesteed.

Vragen om te stellen aan je e-mail dienstverlener

Zeer waarschijnlijk dat je op dit moment al gebruik maakt van e-mail. Het kan dat dit in eigen beheer is of wordt uitbesteed bij een externe hostingpartij. In beide gevallen kan het geen kwaad om (naast het kostenplaatje) op basis van onderstaande vragen eens te inventariseren of jouw e-mailhosting vanuit beveiligingsoogpunt voldoet:

- Is mijn e-mail en mailserverdomein(en) ondertekend met een geldige handtekening (DNSSEC)?
- Zijn mijn e-mail en mailserverdomein(en) voorzien van echtheidswaarmerken tegen e-mailvervalsing (DMARC, DKIM en SPF)?
- Zijn mijn e-mail en mailserverdomein(en) beveiligd e-mailtransport (STARTTLS en DANE)?
- Zijn mijn e-mail en mailserverdomein(en) toegankelijk voor verzenders met moderne IP-adressen (IPv6)?
- Is het e-mail-authenticatieproces versleuteld?

Versleuteling van belangrijk e-mailverkeer

Verstuurd jouw organisatie veel veel gevoelige informatie via e-mail? Dan is het te overwegen een encryptieprotocol te gebruiken, zoals PGP of S/MIME. Beide protocollen kunnen e-mails digitaal ondertekenen, encrypten en vervolgens decrypten. Zo blijft de informatie in e-mails en bijlagen beschermd. Het nadeel van PGP en S/MIME is dat beide partijen (ontvanger en verstuurder) gebruik moeten maken van het encryptieprotocol om met elkaar te communiceren. Ook is de daadwerkelijke gebruik en de implementatie van PGP of S/MIME op on-premise e-mailhosting vrij complex. Daardoor wordt e-mail encryptie nog niet veel ingezet.

Wil je aan de slag met een van deze encryptieprotocollen? Dan zijn er voor zowel PGP als S/MIME verschillende open-source (en betaalde) implementaties te downloaden. Tevens bestaan er vele add-ons en plug-ins voor de meeste moderne internet browsers die het gebruik van e-mailencryptie overal mogelijk maken.

Dit document is gebaseerd op de documenten 'Tips voor het gebruik van e-mail', 'E-mail beveiligingsstandaarden' en 'Geavanceerde informatie over e-mail' van het Digital Trust Center. De originele documenten zijn te vinden via https://www.digitaltrustcenter.nl/tips-voor-het-gebruik-van-e-mail , https://www.digitaltrustcenter.nl/informatie-advies/e-mail/e-mail-beveiligingsstandaarden en https://www.digitaltrustcenter.nl/geavanceerde-informatie-over-e-mail