dhs addsecurity
Email Security
Dienstbeschrijving

Auteur(s): Sander van der Post

Datum: 22 februari 2023
Kenmerk: DB_addsec_esaas_v1_0
Status: Definitief

dhs informatisering
Kanaalstraat 12b
5347 KM Oss
Nederland

0412-653800
info@dhs.nl
www.dhs.nl
kvk 16052550

btw NL008180349B01
Rabobank
iban NL64 RABO 0140440062
swift RABONL2U

adding value

Inhoudsopgave

1 Email Security-as-a-Service

1.1 Introductie

E-mail, we kunnen niet zonder. Dagelijks ontvangen en versturen wij tientallen tot honderden e-mails, om zo onze bedrijfsvoering te ondersteunen. Hoeveel beslissingen maak je wel niet dagelijks op basis van de inhoud van een e-mail? Een opdracht bevestigen, een factuur betalen tot zelfs het bevestigen van contractuele of juridische afspraken. E-mail is een zakelijk communicatie platform, maar wel één die ons soms overspoeld met informatie.

En daar grijpen de cybercriminelen nu precies op in. De overvloed aan e-mails welke dagelijks in onze inbox terecht komt en onze wens (of noodzaak) om al deze e-mails zo snel mogelijk te verwerken. Hoe scherp ben je nog na een drukke dag, om phishing e-mails te herkennen? Hoe oplettend ben je, als je op je smartphone "even snel" je laatste e-mails "wegwerkt"? Tel daar nog eens bij op dat frauduleuze e-mails steeds moeilijker zijn om te herkennen en we trappen er vandaag of morgen allemaal wel een keer in.

Security Awareness trainingen helpen om je scherp en oplettend te houden. Maar ook hier geldt dat we allemaal mensen zijn, en wij maken wel eens fouten. Een beetje technische hulp in het voortijdig afvangen van "verkeerde" e-mails is daarom zeer wenselijk.

E-mail SPAM filters kennen we allemaal al jaren, zowel zakelijk als privé. Maar om de laatste (technische) bedreigingen via e-mail communicatie het hoofd te kunnen bieden, hebben we iets meer nodig. We willen weten:

- Is de afzender wel wie hij zegt dat hij is?
- Komt de email van een betrouwbare bron (e-mail domain / server)
- Zijn alle URL's in de ontvangen e-mail wel veilig?
- Zijn alle attachments in de ontvangen e-mail wel veilig?

Maar ook andersom:

- Verstuur ik niet per ongeluk gevoelige informatie?
- Zijn mijn attachments en URL's wel veilig voor de ontvanger?

Om al deze vragen vroegtijdig te beantwoorden, dus voordat een e-mail überhaupt schadelijk kan worden, zijn technologieën beschikbaar. Technologieën welke vooral gebruikt worden door grote zakelijke ondernemingen (enterprises) of de overheid. Maar iedere organisatie heeft profijt van deze mogelijkheden in het veilig houden van haar medewerkers en bedrijfsdata.

dhs komt om deze reden met de Email Security-as-a-Service dienstverlening. Een dienstverlening die erop gericht is om de e-mail communicatie van en naar uw medewerkers / betrokkenen continu veilig te houden. Ongeacht van welk device je een e-mail verstuurt of ontvangt, ongeacht hoe goed de cybercrimineel ook denkt te zijn, wij houden de inbox schoon en veilig.

1.2 Wat is Email Security

Email Security is het beste te vergelijken met de ouderwetse regels waaraan wij ons "vroeger" moesten houden met het ontvangen en versturen van briefpost.

Voor de verzender betekende dit dat hij moest voldoen aan:

- Het duidelijk vermelden van de ontvanger zijn of haar naam, adres, postcode en woonplaats;
- Het vermelden aan de achterzijde wie of wat de afzender is;
- Het voldoende frankeren van de enveloppe;
- Het deponeren van de brief in de juiste brievenbus;

Simpele regels, waar we wellicht nu om lachen. Enerzijds omdat het ouderwets is natuurlijk. Maar anderzijds omdat iedereen deze regels begreep en kende. Er was weinig ruimte voor het borgen van de "veiligheid" van de ontvanger binnen deze regels, maar dat was "vroeger" ook minder nodig. Je kreeg geen honderden brieven per dag binnen welke je binnen minuten moest (en kon) beantwoorden. En mocht er een frauduleuze brief tussen zitten, dan was dit vrij snel duidelijk en kon er meestal tijdig ingegrepen worden.

Voor e-mails gelden soortgelijke simpele regels ook, om te zorgen dat een e-mail op de juiste plaats aankomt. Echter, zijn deze regels aangevuld met extra beveiligingsmaatregelen. Dit om de ontvanger te helpen te beschermen tegen frauduleuze e-mails. Immers, de impact in een digitale wereld is vele malen groter wanneer er per ongeluk, via een phishing e-mail, gegevens worden gedeeld of schadelijke software wordt binnengehaald.

En dat is nu net wat Email Security continu doet. Het controleren of dat de verzender voldoet aan de basis regels én de aangescherpte beveiligingsmaatregelen bij het versturen van een e-mail.

dhs | Email Security-as-a-Service plaatst zich zelf tussen de ontvanger en verzender en controleert iedere e-mail op meerdere zaken;

- Is de verzender wel diegene die hij zegt dat hij is?
- Komt de e-mail van een veilige en bekende e-mail server?
- Voldoet de verzender (of diens organisatie) aan de beveiligingsmaatregelen, zoals deze zijn vastgelegd in internationale standaarden (SPF, DKIM, DMARC);
- Bevat het attachment dat mogelijk meegestuurd wordt geen virussen of andere schadelijke software?
- Zijn de URL's welke mogelijk meegestuurd wel veilig voor de ontvanger om op te "klikken"?
- Staat de verzender niet op een zwarte lijst van mogelijke cybercriminelen / fraudeurs?

Allen acties waar de ontvanger geen weet van heeft. De e-mail komt, wanneer alle zaken gecontroleerd zijn, gewoon in de inbox terecht. Het zijn nu net de e-mails welke niet "gewoon" in de inbox terecht komen, welke eruit gehaald zijn door het Email Security platform. Dit zijn e-mails die schade hadden kunnen veroorzaken.

1.2.1 Email Encryptie

Ook alle verzonden e-mails vanuit de organisatie worden gecontroleerd, om zo de ontvanger (externen) te beschermen. Hiermee voorkom je dat je als organisatie ooit moet uitleggen waarom je per ongeluk een virus hebt verstuurd.

Maar dat is niet alles. Optioneel, maar beschikbaar binnen de standaard dienstverlening, kun je **email encryptie** aanzetten voor verzonden e-mails.

Het versturen van gevoelige informatie via e-mail is niet altijd wenselijk. Denk bijvoorbeeld aan bankinformatie, gezondheidsinformatie of persoonlijke gegevens (AVG). Toch gebeurt het dagelijks. Soms omdat het "makkelijk" is, soms omdat de verzender gewoon er niet bij stil staat dat hij of zij gevoelige informatie verstuurt.

E-mails zijn te onderscheppen door kwaadwillende. Hiermee krijgen ze potentieel informatie in handen welke als zéér gevoelig kan worden beschouwd. De Email Security oplossing van **dhs** voorkomt dit:

- Het is voor de verzender enorm eenvoudig om, met één druk op de knop, een email versleuteld te versturen;
- Wanneer er per ongeluk toch on-versleutelde gevoelige informatie wordt verstuurd, grijpt het systeem in en versleuteld de e-mail als nog.

De ontvanger krijgt keurig in zijn inbox een melding dat er voor hem een versleuteld bericht klaar staat in een beveiligde omgeving, het beste te vergelijken met "Mijn Overheid Berichtenbox". Daarin kan de e-mail veilig gelezen worden met de wetenschap dat de ontvanger, daadwerkelijk de beoogde ontvanger is.

1.2.2 Optioneel: Email Security Awareness

Additioneel kan er bij de dienst Email Security gekozen worden voor een Email Security Awareness module. Deze module geeft de medewerker de mogelijkheid om geselecteerde security awareness trainingen te volgen in een bekroond online educatie platform.

Deze trainingen kunnen vrijwillig worden gevolgd, of de organisatie kan trainingen toewijzen. Dit laatste gebeurt in overleg en onder begeleiding van **dhs** haar security specialisten, welke ook de rapportages verzorgen over de voortgang van de te volgen trainingen.

Vanuit het security awareness platform worden tevens twee (2) maal per jaar phishing tests opgestart, om zo de medewerkers in de praktijk te toetsen op de door hen vergaarde kennis.

1.3 Waarom "as-a-Service"

Het investeren in, en het up-to-date houden van, enterprise waardige Email Security oplossingen is een kostbare en tijdrovende aangelegenheid voor veel organisaties. Daarbij is er specifieke kennis nodig om beleidsregels en beveiligingsmaatregelen in te richten en te matchen met de bedrijfsvoering van de organisatie.

Toch wordt de behoefte van dergelijke oplossingen met de dag groter, al was het maar omdat het risico met de dag groter wordt dat de organisatie slachtoffer wordt van frauduleuze e-mail communicatie. E-mail communicatie blijft de grootste kans op succes voor kwaadwillende. Het is niet de vraag **of** dat een beveiligingsincident gaat plaatsvinden (via e-mail), maar **wanneer** deze gaat plaatsvinden.

dhs heeft als missie om iedere organisatie zo goed mogelijk te beveiligen tegen dit soort beveiligingsincidenten. Om deze reden heeft **dhs**, in samenwerking met haar partners, een dienst gelanceerd welke het mogelijk maakt om iedere organisatie te voorzien in de best mogelijke Email Security welke er in de markt te verkrijgen is. Breidt dit uit met de optionele Email Security Awareness module, en niet alleen de techniek is geregeld, maar ook de menselijke factor wordt zo goed mogelijk uitgesloten als beveiligingsrisico.

De "as-a-Service" dienstverlening komt vooral tot uiting in het feit dat de organisatie volledig ontzorgd wordt in het beheren en onderhouden van het Email Security systeem. **dhs** en het online platform zorgen voor de benodigde integraties, bewaking en rapportage.

1.3.1 Voordelen

De voordelen van Email Security-as-a-Service ten opzichte van andere oplossingen zijn:

- **Nauwkeurigheid:** De door **dhs** gebruikte technologieën voorzien in een 99,5% nauwkeurigheid, waardoor er meer frauduleuze e-mails gestopt worden dan bijvoorbeeld met Microsoft haar oplossingen;

- **Schaalbaarheid:** Nieuwe medewerkers van de organisatie, of nieuwe shared mailboxen, kunnen direct worden toegevoegd in het online platform, waardoor zij direct beveiligd zijn. Ook het wegvallen van mailboxen of medewerkers, worden verwerkt. Hierdoor wordt er nooit teveel betaald voor de dienst.

- **Encryptie:** Standaard functionaliteit welke beschikbaar is binnen de standaard dienst. Samen met de **dhs** security professionals kan er bepaald worden welke e-mail per definitie altijd versleuteld verstuurd moeten worden.

- **Inline beveiliging:** De oplossing staat tussen de verzender en ontvanger. Er is geen mogelijkheid om ongecontroleerd e-mails te ontvangen of te versturen. Ongeacht op welke locatie de medewerker zijn email verstuurd of ontvangt. Ongeacht op welk device dit gebeurt (laptop, smartphone, tablet..).

- **Multi OS Check:** Veel oplossingen in de markt controleren attachments of URL's voor eventueel schadelijk gedrag binnen Windows of Microsoft Edge. Cybercriminelen worden slimmer en maken virussen specifiek voor bijv. Apple OS of links welke alleen schadelijk zijn wanneer ze geopend worden in Firefox. De **dhs** dienst controleert iedere variabele.

1.4 Inhoud van de dienst

Zoals beschreven is Email Security-as-a-Service een dienst welke, voor een maandelijks bedrag per medewerker en/of shared e-mail account, geleverd wordt aan de organisatie. De initiële installatie, configuratie en opstellen van optionele jaarlijkse Email Security Awareness trainingsplannen, vallen buiten de scope van de "as-a-Service" dienstverlening en worden separaat aangeboden.

dhs biedt de volgende zaken aan binnen de dienst Email Security-as-a-Service:

1. **Email Security Platform**
   dhs maakt voor haar dienstverlening gebruik van een zéér veilig Security Platform van haar partner. De technologie van dit platform is normaliter alleen beschikbaar voor grote organisaties of overheidsinstanties. **dhs** heeft met haar partner een model ontwikkeld, waardoor iedere organisatie gebruik kan maken van dit platform binnen de "as-a-Service" dienstverlening van **dhs**.

   Dit platform biedt de basis van de Email Security-as-a-Service dienstverlening, waarbinnen iedere medewerker inzage kan krijgen in de voor hem of haar tegen gehouden e-mails én optioneel de voor hem of haar relevante Email Security Awareness trainingen kan volgen.

2. **Ondersteuning voor medewerkers**
   Het niet ontvangen van verwachte e-mails kan frustrerend zijn voor medewerkers, zeker wanneer zij niet op de hoogte zijn van de "basis" beveiligingsmaatregelen van de organisatie. Het gebeurt helaas nog regelmatig dat een valide verzender zich onbewust niet aan de internationaal geldende regels houdt, en zijn of haar e-mail daarom niet doorgelaten wordt.

   De **dhs** servicedesk staat klaar voor deze medewerkers om e-mails als nog te beoordelen én zo snel mogelijk vrij te geven aan de ontvanger. Daarbij biedt **dhs** vrijblijvend haar hulp aan, om de verzender te informeren over de geldende beveiligingsmaatregelen.

3. **Beheer en onderhoud**
   Het eenmalig installeren en configureren van een Email Security oplossing is niet afdoende. Dagelijkse beheer is benodigd om een dergelijke oplossing beschikbaar en up-to-date en te houden. Om deze reden biedt de dienst de volgende activiteiten:
   a. **Gebruikersbeheer:** het koppelen en ontkoppelen van gebruikersaccounts / e-mail accounts aan de Email Security oplossing
   b. **Rapportage:** Het op verzoek opleveren van rapportages met betrekking tot e-mail flow, incidenten, etc.
   c. **Support:** Gebruikersvragen of problemen met de Email Security of Email Security Awareness oplossing kunnen rechtstreeks gemeld worden bij de **dhs** servicedesk.

2 Setup en planning

De Email Security-as-a-Service dienstverlening wordt volledig, passend bij de organisatie haar wensen en eisen, geïntegreerd en geconfigureerd. Deze setup dienst kent een eenmalige vaste investering op basis van de "**dhs** Standaard Installatie" definitie. De inhoud van deze installatie procedure is als volgt:

- **Integratie**
  Voor de beste werking van het Email Security, dienen er een aantal integraties plaats te vinden binnen de huidige technische ICT-infrastructuur van de organisatie. De volgende zaken dienen geregeld te worden:
  - Integratie met Microsoft Active Directory / Azure Active Directory ten behoeve van gebruikersaccount en e-mail account integratie;
  - Aanpassingen in de DNS-infrastructuur van de organisatie (@domainnaam.tld) ten behoeve van re-routing van e-mails door de security oplossing heen;
  - Integratie met Outlook clients ten behoeve van de optionele encryptie mogelijkheden.

- **Rapportage periode**
  Voordat de dienst daadwerkelijk geactiveerd wordt, en e-mails door het Email Security platform gecontroleerd worden, zal een zogenaamde rapportage periode ingesteld worden. In deze (vooraf gedefinieerde) periode worden alle e-mails nog doorgelaten richting de ontvangers, echter wordt er alleen gedetecteerd wat er eventueel mis is met deze e-mails.

  Met deze informatie kan de organisatie valide verzenders, informeren over het feit dat hun e-mails niet voldoen aan de internationale beveiligingsstandaarden, met als risico dat deze e-mails in de toekomst "afgevangen" worden.

- **Activatie**
  Wanneer de rapportage periode ten einde is gekomen, zal de dienst geactiveerd worden. Per direct worden alle inkomende en uitgaande e-mails gecontroleerd. De organisatie heeft op dat moment wederom een belangrijke stap gezet in haar digitale veiligheid.

3 Dienstverlening dhs

Voor alle diensten beschreven in dit document, als ook overige diensten geleverd door **dhs** onder de merknamen van **dhs addcloud**, **dhs addcontrol**, **dhs addwireless**, **dhs addsecurity, dhs addmobility** en **dhs addbackup**, geldt dat deze onderhevig zijn aan een onderliggende "Service Level Agreement (SLA)". Deze Master SLA is opvraagbaar bij **dhs** en/of te downloaden via de website van **dhs** (www.dhs.nl).

4 Contractduur, looptijd en verlenging

De dienst **dhs** Email Security-as-a-Service wordt u aangeboden als een abonnement met een bepaalde contractlooptijd.

- Standaard wordt deze overeenkomst aangegaan voor een periode van 36 maanden;
- De overeenkomst is niet tussentijds opzegbaar, maar wel aanpasbaar in aantallen;
- Opzegging dient schriftelijk en uiterlijk 2 maanden voorafgaande aan einddatum te geschieden;
- Indien geen opzegging heeft plaatsgevonden wordt de overeenkomst automatisch met een periode van 12 maanden verlengt;

Overige bepalingen en voorwaarden staan beschreven in de onderliggende Service Level Agreement (Master SLA).