Beleid mailen met de politie (2023)

Bestemd voor partners van politie

Werkgroep Veilig Mailen

Definitief

Versie 1.4
19 mei 2023

Rubricering Niet vertrouwelijk

« waakzaam en dienstbaar »

Deze notitie is een toelichting op het beveiligingsbeleid voor het gebruik van e-mail door de politie. E-mail wordt niet gegarandeerd afgeleverd en om misbruik te voorkomen zijn er maatregelen om ongewenste berichten te blokkeren. Deze informatie is bestemd voor partners en ICT-dienstverleners van de politie

1. Waarom beveiligen van e-mail

Overheden en burgers kunnen veel schade van cybercriminaliteit ondervinden. Door onbeveiligde websites en via e-mail kunnen gevoelige gegevens in verkeerde handen vallen. Via malware (virussen) kan er schade toegebracht worden aan informatiesystemen, waaronder het uitvallen van systemen. Ook kan dit ervoor zorgen dat gevoelige gegevens bij de verkeerde ontvanger terecht komen. Phishing mails, (je voordoen als een ander), die verstuurd worden uit naam van officiële instanties kunnen het vertrouwen van de burger in de overheid behoorlijk ondermijnen. Moderne internetstandaarden helpen cybercriminaliteit te voorkomen. Deze standaarden staan verderop in dit beleid toegelicht.

2. Forum Standaardisatie en NCSC

De politie is verplicht, net als alle andere (semi)overheidsorganisaties, om de internetstandaarden van het Forum Standaardisatie te implementeren. Het Forum Standaardisatie is een overheidsorganisatie die voor de rijksoverheid de beveiligingsstandaarden onderzoekt en vaststelt. Als partner van de politie moet u aan dezelfde standaarden voldoen om e-mail met de politie te kunnen uitwisselen. De belangrijkste standaarden zijn:

- (Start)TLS en DANE (beveiligde verbindingen) (NCSC TLS richtlijn)
- DNSSEC (domeinnaambeveiliging)
- SPF, DKIM en DMARC (anti-phishing/-spoofing)

Het Nationaal Cyber Security Centrum (NCSC) adviseert de overheid en de markt over de inzet van deze standaarden bij het gebruik van e-mail via internet.

3. Welke beveiligingsmaatregelen gebruikt de politie?

De politie gebruikt de volgende methoden om het inkomende mailverkeer te beveiligen:

Internet Mail

1. **Viruscontrole**: Het verkeer tussen domeinen wordt geïnspecteerd op virussen, malware en ongeautoriseerde toegang. Alleen bestanden die gecontroleerd kunnen worden, worden doorgelaten. Malware en programma's (exe en bin) worden in Quarantaine geplaatst.
2. **Encryptie**: Verbindingen met mailservers worden beveiligd met encryptie. De afkomst van de mail wordt gecontroleerd en gegevens worden beveiligd tegen afluisteren.
3. **Ongewenste mail:** Al het inkomende verkeer wordt gecontroleerd op Spam, DDOS, Spoofing en Phishing.

Alternatieven

1. **Partnerkoppeling**: Mail van partners wordt via een specifieke partnerkoppeling via vertrouwde netwerken gerouteerd.
2. **Grote bestanden**. Voor bestanden groter dan 20MB en voor bestanden die niet veilig gemaild kunnen worden wordt geen mail maar een uitwisselingsplatform (bu.politie.local) gebruikt. Alleen de politie kan een partner een uitnodiging voor dit platform sturen.

Beleid voor virussen en anti-malware

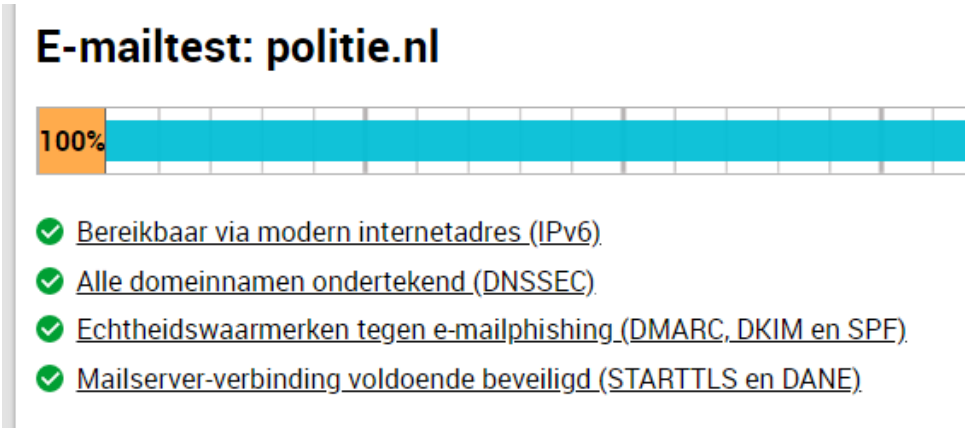
Voor het controleren en filteren wordt al het inkomende verkeer gecontroleerd. Alleen berichten die geïnspecteerd kunnen worden, worden doorgelaten. Alle andere worden gestopt, zoals:

- Malware en virussen
- Actieve componenten, zoals macro's in Office-documenten (Word, Excel).
- Berichten beveiligd met een wachtwoord
- Onbekende extensies of binary
- Encrypted berichten

Beleid voor encryptie, spam, phishing en spoofing

Voor de instellingen van de mailserver volgt de politie het *Forum Standaardisatie*. De instellingen van uw mailserver kunnen getest worden bij Internet.NL.

In de richtlijn **"Veilig mailen politie**" staat de controle uitgelegd.



4. Afhandeling van berichten

Berichten die u naar de politie stuurt worden als volgt afgehandeld:

1. **Doorgelaten**: Berichten die voldoen aan het beleid worden afgeleverd bij de geadresseerde.
2. **Quarantaine**. Het bericht wordt binnengelaten en gecontroleerd. Als het niet voldoet aan het beleid voor virussen en anti-malware, wordt het in quarantaine geplaatst. De geadresseerde van politie krijgt een mail dat het bericht niet afgeleverd kan worden en kan met u contact opnemen.
3. **Blokkeren**. Berichten die niet voldoen aan het beleid van de politie worden geblokkeerd. De geadresseerde politiemedewerker krijgt hiervan **geen** bericht. U als afzender krijgt, afhankelijk van uw mailserver, een foutmelding. Hiervoor is de politie niet verantwoordelijk.

5. Alternatieven

Partnerkoppelingen

Mailservers van overheidspartners van de politie met een specifieke partnerkoppeling worden niet via Internet verstuurd. Deze maildomeinen staan in de Omegalijst en zijn door een politiemedewerker op het Intranet te raadplegen.

Bestandsuitwisseling (bu.politie.local)

Als u als partner niet aan de e-mailstandaard van de overheid kan voldoen, of de bestanden zijn te groot, of er zijn andere redenen, dan kan u als partner uw contactpersoon bij politie verzoeken om gebruik te maken van de dienst bestandsuitwisseling. De politie bepaalt de inzet van deze dienst. Neem hiervoor contact op met uw contactpersoon bij de politie.

6. Standaarden

Hieronder de standaarden die gevolgd moeten worden. Neem contact op met uw IT verantwoordelijke of de veilige emailconstructies bij uw organisatie mogelijk zijn of niet.

Standaard	Beleid
SPF (Sender Policy Framework)	SPF wordt gebruikt om te controleren of de afzender van een e-mailbericht overeenkomt met de verzendende mailserver op basis van domeingegevens. In deze domeingegevens staat een beleid aangegeven hoe om te gaan met mail afkomstig van een verkeerde mailserver.
DKIM (DomainKeys Identified Mail Signatures)	DKIM wordt gebruikt om te verifiëren of een e-mailbericht afkomstig is van een mailserver behorende bij het afzenderdomein (bijvoorbeeld @politie.nl). DKIM maakt hiervoor gebruik van de “digitale handtekeningen” die gecontroleerd kunnen worden door middel van domeingegevens.
DMARC (Domain-based Message Authentication, Reporting and Conformance)	DMARC is een aanvulling op SPF en DKIM. Ook bij DMARC wordt door middel van beleid aangegeven wat er moet gebeuren met onjuiste e-mails. Daarnaast wordt DMARC gebruikt voor het genereren van rapporten omtrent de resultaten van SPF en DKIM.
DNSSEC (Domain Name System Security Extensions)	DNS is kwetsbaar waardoor een kwaadwillende een domeinnaam kan koppelen aan een ander IP-adres ("DNS spoofing"). Gebruikers kunnen hierdoor bijvoorbeeld worden misleid naar een frauduleuze website. DNS Security Extensions (DNSSEC) lost dit op.
TLS (Transport Layer Security)	TLS is een protocol dat tot doel heeft om beveiligde verbindingen (encryptie) op de transportlaag over het internet te verzorgen. Dit biedt een beveiligde basis, waar de applicatie protocollen als HTTP (webverkeer) of SMTP en IMAP (mailuitwisseling) gebruik van kunnen maken.
STARTTLS en DANE (SMTP Service Extension for Secure SMTP over Transport Layer Security (STARTTLS) en SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE)	STARTTLS in combinatie met DANE gaat het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen.

Informatie

Forum	Forum Standaardisatie
Forum Standaardisatie	https://www.forumstandaardisatie.nl
Lijst verplichte standaarden	https://forumstandaardisatie.nl/open-standaarden
Checklist	https://forumstandaardisatie.nl/open-standaarden/verplicht
Platform Internetstandaarden Test mailserver	https://internet.nl/
NCSC	**Nationaal Cyber Security Centrum**
NCSC	https://www.ncsc.nl/
TLS	https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging

Communicatie

Voor meer informatie kunt u zich wenden tot uw contactpersoon bij de politie