Algoritmebeschrijving

Algoritme: Veilig mailen van Gemeente Wijchen

Algemene informatie

Naam
Veilig mailen

Korte omschrijving
Dit algoritme helpt e-mailgebruikers te bepalen wanneer een e-mail gevoelige informatie bevat en beveiligd moet worden verstuurd.

Organisatie
Gemeente Wijchen

Thema
Organisatie en bedrijfsvoering

Status
In gebruik

Begindatum
2023-01

Contactgegevens
gemeente@wijchen.nl

Link naar publiekspagina
https://www.druten.nl/over-deze-website

Publicatiecategorie
Overige algoritmes

Verantwoord gebruik

Doel en impact
Het doel van dit algoritme is bijdragen aan goede beveiliging van e-mails die verzonden worden. Niet te weinig beveiliging, maar ook niet te veel. Het algoritme wijst verzenders van een e-mail op gevoelige informatie en moedigt hen aan die veilig te verzenden. Dat kan door encryptie, tweefactorauthenticatie voor de ontvanger, intrekmogelijkheid en logging. Ongevoelige informatie blijft eenvoudig toegankelijk. Het algoritme heeft geen invloed op de materiële rechtspositie van inwoners of bedrijven.

Afwegingen

Het beoordelen van e-mails door een algoritme is effectiever dan met een door de mens gemaakte woordenlijst of indeling. Het algoritme heeft geen invloed op de inhoud van een e-mail.

Menselijke tussenkomst

De medewerker van de gemeente kiest zelf om een e-mail wel of niet beveiligd te verzenden. Het algoritme doet hier alleen een aanbeveling in.

Risicobeheer

De leverancier houdt de prestaties van het algoritme bij. De leverancier merkt het als het algoritme fouten maakt en past het aan. De gemeente kan op een dashboard de prestaties van het algoritme volgen.

Toelichting op impacttoetsen

Er is voorafgaand aan de implementatie van de software een Data Protection Impact Assessment (DPIA) uitgevoerd.

Werking

Gegevens

Het algoritme is gebaseerd op geanonimiseerde historische berichten in combinatie met of deze berichten wel of niet veilig verzonden zijn. De anonimisering wordt in meerdere stappen gedaan, waarbij alleen aggregaten over vele duizenden berichten opgeslagen worden. Daarnaast worden persoonsgegevens geautomatiseerd uit de data verwijderd. Hiermee is de data geanonimiseerd en zijn de originele berichten onmogelijk uit de data te halen.

Technische werking

Bij het samenstellen van een nieuwe e-mail wordt op basis van de termen in het bericht en de bijlagen gekeken hoe vergelijkbaar dit is met eerder (veilig of normaal) verzonden e-mails. Als de e-mail voldoende vergelijkbaar is met berichten die normaal gesproken veilig verzonden worden, wordt de e-mail als potentieel gevoelig gemarkeerd. Op basis van de terminologie in de e-mail wordt bepaald of deze relateert aan een specifieke categorie van gevoelige informatie. Bijvoorbeeld bepaalde persoonsgegevens zoals medische informatie over personen. Op het moment dat de e-mail als gevoelig is geclassificeerd en over een onderwerp gaat waarvan de organisatie heeft ingesteld dat dit veilig verzonden moet worden, krijgt de gebruiker een aanbeveling om de e-mail veilig te verzenden.

Leverancier

Zivver. Het algoritme wordt geleverd via ICT Rijk van Nijmegen (iRvN) en gebruikt door alle Rijk van Nijmegen gemeenten.

Metadata

Taal

nld

Versie publicatiestandaard

1.0

Zoektermen

- Zivver
- Veilig e-mailen