PROBLEEM?

- Sinds mei 2018 zijn de nieuwe Europese GDPR-richtlijnen van kracht (General Data Protection Regulation)
- Hierdoor is een e-mail met "gevoelige" informatie (zoals medische gegevens) versturen is een datalek geworden

Sla de technische uitleg over en ga direct naar de oplossing!

GEËNCRYPTEERDE E-MAILS VERSTUREN MET KLASSIEKE OPLOSSINGEN?

Courante e-mail programma's zoals Outlook en Thunderbird laten toe e-mails te encrypteren maar dit enkel op voorwaarde dat **beide partijen** redelijk technische handelingen uitvoeren.

- **Verzender en de ontvanger** moeten verstaan hoe publieke en private encryptie sleutels werken
- **Verzender en de ontvanger** moeten elk een "key pair" genereren en hun eigen publieke key versturen naar de andere persoon
- **Verzender en ontvanger** moeten hun private encryptie sleutel veilig bijhouden zodat ze niet gecompromitteerd wordt of verloren gaat. Moest deze toch verloren gaan verlies je de toegang tot de e-mails!
- **Verzender en ontvanger** moeten hun herroepingscertificaat veilig bijhouden omdat hun openbare sleutel hiermee ongeldig kan worden gemaakt als hun private sleutel verloren is geraakt
- **Verzender en ontvanger** moeten hun private sleutel beveiligen met een wachtwoord dat niet het zelfde is als dat van de e-mail account
- **Verzender en ontvanger** moeten overeenkomen om de zelfde encryptie standaard te gebruiken voor de e-mails (PGP, S/MIME, …)

Eens dit alles in orde is kan je beginnen zoeken naar de browser extension, smartphone app of "e-mail client plugin" die je zou willen gebruiken voor de feitelijke encryptie.

Zelfs als al deze punten door verzender en ontvanger correct uitgevoerd worden kunnen de "headers" van de e-mails nog gelezen worden waarin staat wie naar wie stuurt over welk onderwerp.

Ver van ideaal dus als je kijkt naar het gebruiksgemak!

E-MAILS & ATTACHMENTS OPSLAAN OP EEN SERVER BUITEN DE EU?

De GDPR verplicht gebruikers niet om data op servers in de EU op te slaan **maar** er zijn **extra vereisten** waaraan voldaan moet worden als de servers buiten de EU liggen.

1. Je moet een legitieme reden hebben om de data buiten de EU op te slaan
2. Je moet de toelating hebben van de persoon van wie de data buiten de EU wordt opgeslagen
3. Je moet die persoon de optie geven om dit te weigeren (opt-out)

DE OPLOSSING - HOE WERKT HET?

1. De verzender verstuurt een wachtwoord naar de ontvanger via telefoon, SMS, Skype, … (niet via ongeëncrypteerde "normale" e-mail)

2. De verzender verstuurt vanuit een online geëncrypteerd e-mail platform een e-mail naar de ontvanger
3. De ontvanger krijgt een link via "normale" e-mail
4. De ontvanger logt via die link in op het geëncrypteerde e-mail platform waar hij/zij geëncrypteerde e-mails kan lezen en versturen.

DE OPLOSSING – VOORDELEN

1. **GDPR compliant** (alles is geëncrypteerd en de servers staan in Duitsland)
2. Absoluut **minimale inspanning** vereist van de verzender en ontvanger
3. De ontvanger heeft geen eigen betalende account nodig op het platform
4. Alle **e-mails** worden automatisch voor verzender en ontvanger **geëncrypteerd opgeslagen**
5. Alle **Attachments** worden **geëncrypteerd opgeslagen**
6. Zelfs de e-mail header informatie is geëncrypteerd
7. E-mails blijven permanent toegankelijk, ook voor de ontvanger die geen eigen betalende account heeft op het platform
8. Nieuwe E-mail **notificaties** kunnen ontvangen worden via de online e-mail client in **elke browser** of op een **smartphone** of **tablet** (Android en iOS)
9. Als verzender heb je ook de optie om met één klik niet geëncrypteerde e-mails te versturen.
   Deze worden geëncrypteerd opgeslagen op het platform gebruikt door de verzender maar komen ongeëncrypteerd toe in de inbox van de ontvanger

DE OPLOSSING – NADELEN

1. Geëncrypteerde mails versturen kan via het online platform (in de browser) of via smartphone of tablet (Android en iOS) maar niet via Outlook of Thunderbird

DE OPLOSSING – WIE VERZORGT HET?

Het online geëncrypteerde e-mail platform dat gebruikt wordt als oplossing is tutanota.com
Je wordt rechtstreeks bij Tutanota klant voor de afname van deze dienst.

Bij Webaholic kan je terecht voor het diestenpakket "Geëncrypteerde e-mail":

- De initiële setup van de Tutanota account
- Het koppelen van een domeinnaam aan de Tutanota account waardoor je **een gepersonaliseerd e-mail adres** kan gebruiken.
  Ex: voornaam@achternaam.be of contact@bedrijfsnaam.com
- Hands-on opleiding via remote support bij de eerste ingebruikname
- Gratis support gedurende de eerste week

Dit dienstenpakket kost éénmalig **75 € excl.**, de domeinnaam kost **12 € / jaar excl.** (*) tenzij u deze reeds bezit.

(*) *Opgelet, deze lage prijs geldt voor .be, .com, … maar niet voor sommige exotischere en dus duurdere domein namen zoals .gent, .vlaanderen, …. Contacteer me gerust voor meer informatie!*

U kan me contacteren via e-mail op webmaster@webaholic.be of via GSM op 0486/246882

Met vriendelijke groet,
Manuel Schroyens