# HTTP & HTTPS

## Hoe werkt deze techniek?

HTTP staat voor HyperText Transfer Protocol en is de basis van het internet. Het zorgt ervoor dat jouw browser en een webserver met elkaar kunnen praten. Wanneer jij een website bezoekt, stuurt jouw browser een verzoek naar de server met de vraag om bijvoorbeeld een webpagina, afbeelding of video te laten zien. De server verwerkt dit verzoek en stuurt vervolgens een antwoord terug. Dit heet een response. HTTP is dus eigenlijk een soort taal die ervoor zorgt dat informatie wordt uitgewisseld tussen gebruiker en website. Het nadeel van HTTP is dat alle gegevens in gewone tekst worden verstuurd. Dat betekent dat anderen op hetzelfde netwerk kunnen meekijken of zelfs informatie kunnen aanpassen.

Om dat probleem op te lossen, bestaat er HTTPS. De S staat voor secure, wat betekent dat de verbinding beveiligd is. HTTPS gebruikt een techniek die TLS heet (Transport Layer Security). Daarbij wordt alle data versleuteld, zodat niemand meer kan meelezen. Dit werkt met digitale certificaten. Zo'n certificaat vertelt de browser wie de website is en bevat een publieke sleutel om de verbinding veilig te maken. De browser controleert of dit certificaat betrouwbaar is en of het hoort bij de juiste website. Pas als alles klopt, wordt de beveiligde verbinding opgezet. Dankzij deze techniek kunnen we vandaag de dag veilig online bankieren, inloggen of persoonlijke gegevens invullen zonder dat anderen kunnen meekijken.

## De geschiedenis

- **1991**: HTTP werd geïntroduceerd door Tim Berners-Lee, de uitvinder van het World Wide Web. De eerste versie was heel simpel en bedoeld voor het uitwisselen van tekst.

- **1994-1996**: opvolgende versies van HTTP verschenen (1.0 en 1.1), met meer functies en betere prestaties.

- **1994**: Netscape ontwikkelde SSL, waardoor de eerste veilige verbindingen mogelijk werden (HTTPS). Dit was vooral bedoeld voor online betalingen.

- **2015**: HTTP/2 werd geïntroduceerd, sneller en efficiënter.

- **2022**: HTTP/3 is in opkomst, gebaseerd op QUIC, dat nog sneller en stabieler werkt.

## Wat is er stuk?

Eigenlijk is het bij dit onderwerp vrij makkelijk om te concluderen dat http stuk is. Zoals eerder gezegd zit er op deze protocollen geen beveiliging. Het risico is dat hierdoor gegevens zoals wachtwoorden en andere persoonlijke informatie kunnen worden onderschept.

Daarnaast is HTTPS alleen een versleuteling van de verbinding, het beschermt dus niet tegen alles. Als een website zelf slecht beveiligd is, bijvoorbeeld door zwakke wachtwoorden, lekken in de code of malware, kan een hacker alsnog toegang krijgen tot gegevens. Ook gebruikers kunnen in de problemen komen als ze waarschuwingen negeren of op onbetrouwbare links klikken. Verder kunnen sommige oudere websites of apparaten nog steeds verouderde versies van TLS gebruiken, die kwetsbaar zijn voor aanvallen. HTTPS maakt het internet dus veel veiliger, maar het is geen garantie voor volledige veiligheid. Het werkt goed zolang certificaten betrouwbaar zijn, servers goed zijn ingesteld en gebruikers voorzichtig omgaan met wat ze online doen.

Beveiligen is altijd goed, maar is https dan onbreekbaar? Het korte antwoord is nee. In de praktijk blijkt namelijk bijna geen enkel systeem 100% veilig. Als een website verkeerd is ingesteld, een certificaat onterecht wordt uitgegeven of een gebruiker malware op zijn computer heeft, kan de beveiliging alsnog worden omzeild. Ook kunnen aanvallers proberen oude, zwakkere versies van TLS af te dwingen. In de praktijk is HTTPS echter wel zeer betrouwbaar: het maakt het voor hackers vrijwel onmogelijk om verkeer af te luisteren of te manipuleren. Je kunt dus zeggen dat HTTPS niet onbreekbaar is, maar wel het sterkste en meest betrouwbare systeem dat we op dit moment hebben om internetverkeer te beveiligen.

## Hoe kunnen we het repareren?

Eigenlijk is het door de introductie van https al gerepareerd. Hierdoor zijn de grootste beveiligingsrisico's al ingeperkt. Daarnaast krijg je op veel browsers ook al een melding als je een website probeert te betreden die gebruik maakt van http. Je zou dus kunnen concluderen dat het al zo goed als gerepareerd is.

## Persoonlijke reflectie op onderzoek

Met dit onderzoek vond ik het interessant om meer te weten te komen over dit onderwerp. Mijn vader werkt in de IT en gebruikt vaak vergelijkbare termen, maar hij praat daar meestal in vakjargon over, waardoor ik het moeilijk vond om te volgen. Door dit onderzoek begrijp ik nu beter waar hij het over heeft en kan ik in ieder geval meepraten over de basis van HTTP en HTTPS. Vooraf wist ik wel dat HTTP-websites niet goed beveiligd waren, maar niet precies wat de risico's daarvan waren of hoe hackers daarvan kunnen profiteren. Nu begrijp ik dat onbeveiligde verbindingen gevoelige gegevens kunnen blootstellen en dat HTTPS dit grotendeels oplost door data te versleutelen. Ik vond het ook verrassend om te leren hoe certificaten werken en hoeveel stappen er nodig zijn om een verbinding echt veilig te maken. Daardoor zie ik nu beter hoeveel er achter iets simpels als "een website openen" zit. Wat ik moeilijk vond, was om te bedenken hoe we HTTP konden repareren, omdat dit in feite al is gebeurd met de komst van HTTPS. Wel merk ik nu dat beveiliging nooit helemaal klaar is. Vanaf nu let ik beter op of websites een HTTPS-certificaat hebben en begrijp ik waarom dat zo belangrijk is.

## Persoonlijke reflecties op de presentaties

### Onderwerp het Fediversum

Doordat wij les hebben gehad over dit onderwerp en meneer De Zwart enthousiast over dit onderwerp vertelde wist ik al aardig wat van het fediversum. Ik wist dat het een soort decentraliseert alternatief was op de bekende social media. Wat ik nog niet wist is hoe activity pub werkt, dus het was erg goed dat dit verder toegelicht werd. Daarnaast wist ik wel dat je data niet doorverkocht werd, maar niet dat het alleen bij de instantie blijft waar je gebruik van maakt. Een andere nuttige functie is dat je bij apps van het Fediversum moderators kan kiezen die bepalen wat er in je tijdlijn voorbij komt. Het geen wat mij aan het denken heeft gezet is dat het ook bij de big tech social media handig zou zijn als je b.v.b met je Snapchat account berichten kan sturen naar een Instagram gebruiker.

### Onderwerp Social media algoritmes:

Doordat ik al jaren bezig ben met het groeien van Instagram pagina's heb ik me al heel veel ingelezen over dit onderwerp, want als je het algoritme begrijpt kan je hier op inspelen. Ik wist dus al hoe ze werken en hoe ze vroeger werkten. Wat ik nog niet wist is dat Facebook het platform was dat de hedendaagse variant van een tijdlijn introduceerde. Daarnaast kende ik de term filterbubbel niet, ik wist na de uitleg wel wat het betekende alleen had ik de term nog niet eerder gehoord. Het heeft mij ook aan het denken gezet, omdat je een beetje in je eigen realiteit gaat leven. Dit komt omdat je meer krijgt te zien van het geen wat je interesseert en hierdoor kan je een beetje gaan doorslaan in wat je denkt over bepaalde onderwerpen.

### Onderwerp Generative ai

Over dit onderwerp dacht ik eerst: Wat wordt hiermee bedoeld'', echter toen Kaoutar en Zakaria gingen uitleggen over het onderwerp klonk het spannender dan het daadwerkelijk is. Daarentegen heb ik wel geleerd dat de ai's eigenlijk met elkaar communiceren. Hiermee bedoelen ze dat AI's elkaars output kunnen gebruiken om beter te worden, bijvoorbeeld: de ene AI maakt een afbeelding, en een andere AI

controleert of die afbeelding er realistisch uitziet. Zo leren ze samen en verbeteren ze elkaars resultaten. Dit heeft mij ook aan het denken gezet, dat het ook een beetje triest is voor die mensen dat ze daarvoor ‘’misbruikt’’ worden.  Wat me ook is bijgebleven, is dat veel AI-systemen nog steeds afhankelijk zijn van menselijke controle. Foto’s en data worden vaak gecontroleerd door mensen in lage lonen landen. Dat vond ik best erg, omdat die mensen soms slecht betaald worden voor eentonig werk. Ik was mij er niet van bewust dat er ook nog veel mensen gebruikt worden om de ai op deze manier te ‘’controleren’’.

## Onderwerp Datacentres

Ik wist door mijn schoonvader, die in de datacenters werkt, al het een en ander over dit onderwerp, maar ik had nooit echt nagedacht over hoe de onderdelen precies samenwerken en hoe de koeling in zo’n centrum werkt. Het zette mij wel aan het denken dat water, iets wat je normaal niet met stroom combineert, juist een belangrijke rol speelt bij het koel houden van de servers. Tijdens de presentatie werd goed uitgelegd hoe belangrijk die koeling is om storingen te voorkomen en hoe veel energie dat kost. Wat me ook aan het denken heeft gezet, is dat datacenters verantwoordelijk zijn voor ongeveer 1 à 2 procent van het wereldwijde stroomverbruik. Dat laat zien hoeveel impact deze datacenters hebben op het milieu. Ik vond het interessant om te horen dat er steeds meer wordt gewerkt aan duurzame oplossingen, zoals het hergebruiken van restwarmte of het inzetten van groene energie. Toen ik dit hoorde dacht ik namelijk direct; maar hoe is dit dan te voorkomen? De presentatie heeft me laten inzien dat achter iets simpels als het opslaan van data een enorm netwerk van datacenters schuilt.