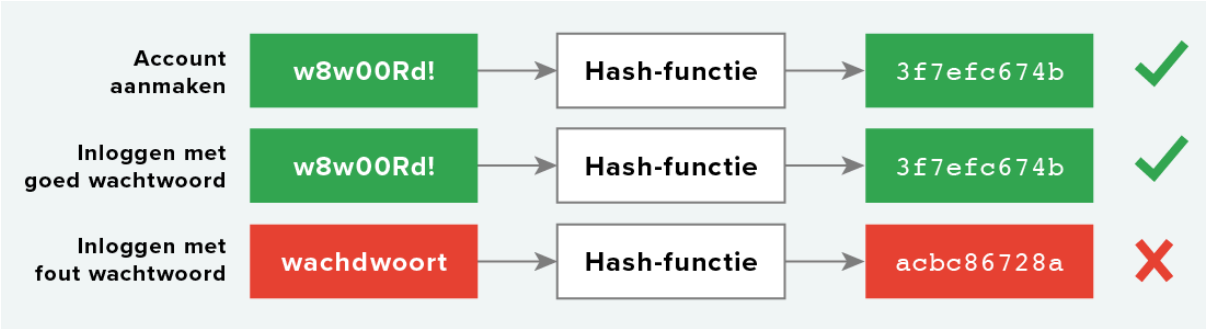
Technologie speelt een grote rol in de samenleving, en criminelen proberen op allerlei manieren jouw gegevens te krijgen. Er zijn hackers die hacken met goede, en met slechte bedoelingen. Mensen willen vaak je gegevens hebben omdat ze daar geld mee kunnen verdienen door het bijvoorbeeld te verkopen aan andere bedrijven die dan beter advertenties aan jou kunnen laten zien. Digitale beveiliging is alle manieren waarop je gegevens beveiligd kunnen worden. Zelf kan je je eigen veiligheid ook vergroten door bijvoorbeeld een beter wachtwoord te gebruiken. **Authenticatie** (ook wel identificatie) is een controle om te kijken of een gebruiker toegang mag hebben tot bepaalde gegevens, dat is vaak iets dat je weet (wachtwoord), hebt (pas), of bent (vingerafdruk). Verificatie is het deel waar ze vragen of je wel bent wie je zegt te zijn. 2-stap verificatie (two factor authentication) is als je iets dat je weet, en iets dat je hebt nodig hebt om in te loggen (bijv je wachtwoord en je telefoon om in te loggen op een computer). Screening is als met bijvoorbeeld camera's mensen of voertuigen worden geïdentificeerd, dit wordt vaak gebruikt door de overheid

Gegevens moeten aan bepaalde eisen voldoen en integer zijn, op bijvoorbeeld een school mogen alleen sommige mensen bepaalde gegevens verwerken. Checksum is een lange rij met letters en cijfers die bij een bestand hoort, en als het bestand veranderd wordt dan verandert de checksum ook, zo kan je dus kijken of je bestand integer is en niet veranderd is. Back-ups zijn handig om zeker te zijn dat je een integer bestand hebt want als er iets mee gebeurt heb je de oude versie nog. Experts raden het volgende aan: zorg er altijd voor dat er drie kopieën van de gegevens zijn, die op minimaal twee verschillende manieren worden opgeslagen, waarvan één kopie op een andere locatie wordt bewaard. Op deze manier gaat niet alles weg als er bijvoorbeeld een brand is op één plek. Encryptie is als je met iets van een wachtwoord een bestand nutteloos kan maken voor hackers. Het wordt altijd op dezelfde manier gehusseld dus kan je wel checken of 2 dingen hetzelfde zijn

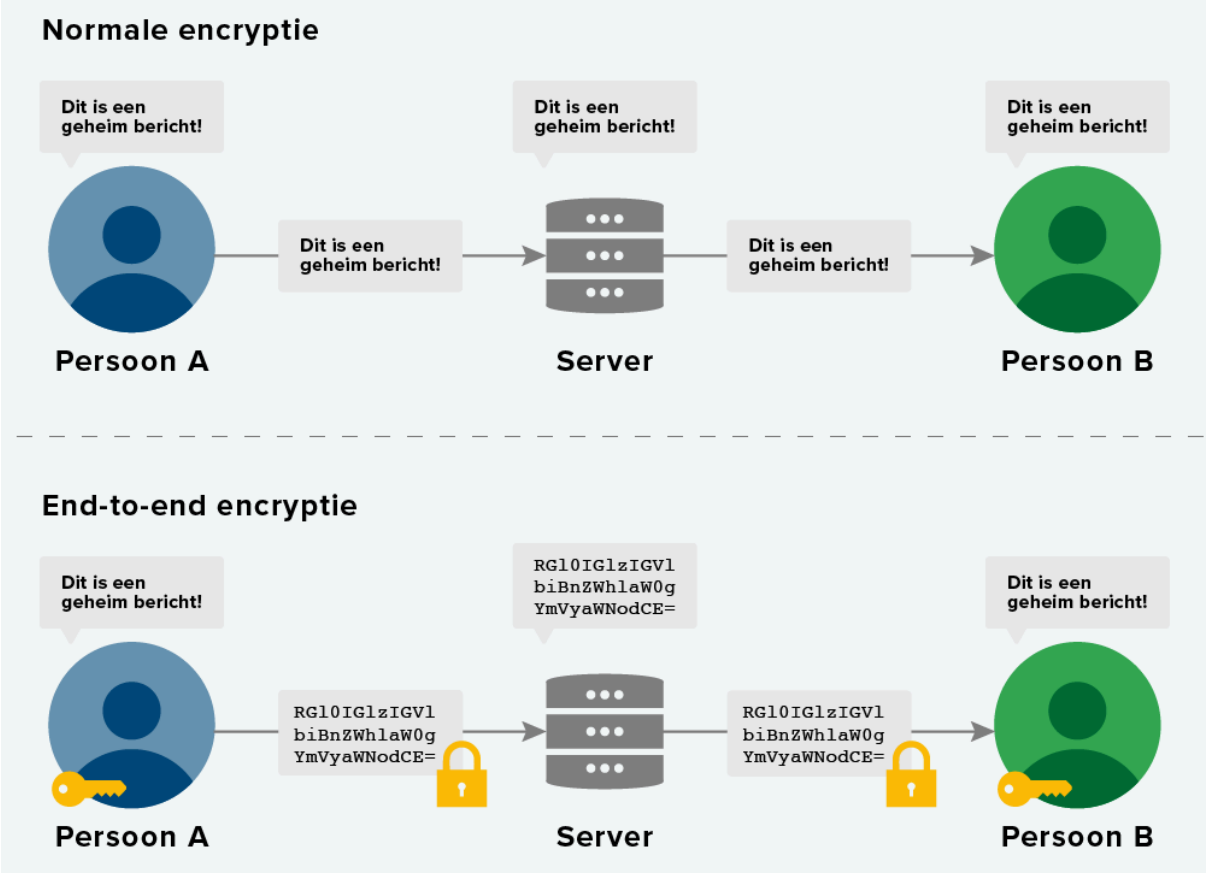



Een DDoS (Distributed Denial Of Service) kan ervoor zorgen dat een service niet meer werkt, dit gebeurt omdat mensen de website crashen door heel veel aanvragen te doen en het te overloaden. Dit is strafbaar en op het dark web kan je mensen betalen om zijn aanval uit te voeren. Al die aanvragen worden gedaan door computers die als zombies zijn voor de aanvaller. Je kan dit tegengaan door bijvoorbeeld te filteren wat wel of niet mag gebeuren in het verkeer van je website.

## Bedreigingen

Een zwakheid in de architectuur maakt gebruik van een tekortkoming in een van de drie lagen in een computer (fysiek, logisch, toepassingen), of in de communicatie tussen twee lagen. Hierdoor kunnen mensen bijvoorbeeld toegang krijgen tot je camera zonder dat je daar toestemming voor geeft. Als iemand zo'n zwakheid heeft gevonden is dat een lek. Als je de vraag vanuit de app naar de database aan kan passen kan je meer gegevens zien dan

dat hoort en die aanpassen. Dat is een SQL injectie. Je kan dus instructies schrijven terwijl je eigenlijk alleen tekst hoorde te kunnen schrijven. Ethische hackers proberen dit vaak ook.
Een man-in-the-middle aanval is als iemand tussen de connectie van bijvoorbeeld jou en een website komt, terwijl het eigenlijk rechtstreeks hoort te gaan. Dit is waarom openbare WiFi gevaarlijk kon zijn, de eigenaar van de hotspot werd dan de man in the middle. De S in HTTPS staat voor secure, en als je https hebt zijn je verstuurde gegevens versleuteld. HTTP is nu verplicht en dus is het nu niet meer gevaarlijk om verbinding te maken met openbare WiFi. Voor HTTPS moet je een SSL-certificaat installeren. Daarmee weet de cliënt wie de server bestuurt en is het dus niet meer anoniem. Zo'n certificaat moet worden aangevraagd bij een centrale organisatie. De eigenaar van de website moet dan bij zo'n organisatie zichzelf verifiëren.
Als dat gedaan is komt er ook een slotje links van de adresbalk. End to End encryptie wordt niet ongecodeerd opgeslagen op het internet




Zwakke wachtwoorden zijn slecht omdat mensen met een brute-force programma duizenden wachtwoorden in een seconde kunnen proberen, en die programma's beginnen meestal met dingen als Wachtwoord123, niet 6ukk)0Ple. Hoe sterker de computer van de aanvaller is, hoe meer wachtwoorden hij snel kan gokken. Veel websites proberen dit tegen te houden door iemand bijvoorbeeld maar 10 keer te laten proberen om een wachtwoord in te voeren, maar aanvallers vinden hier vaak manieren tegen
Social engineering is als men psychologische trucs gebruikt om achter je wachtwoord te komen, dit doe je vaak door voor te doen als iemand die je vertrouwt. Vaak via e-mail of telefoon.
Phishing is als je naar een website wordt gelokt die erg op een andere website lijkt (zoals je bank), en als je dan inlogt heeft de aanvaller je inloggegevens. Phishing kan je opmerken aan bijvoorbeeld taalfouten of dat je een link moet klikken in de mail.

Malware is alle software die kwaad zinnig is bedoeld. Bij een Trojan horse heeft iemand niet door dat wat hij/zij download malware is, de persoon heeft dan bijvoorbeeld iets van een chat-bijlage gedownload. Een worm is een type malware die zichzelf verspreidt naar andere computers als het op de eerste computer komt, door bijvoorbeeld naar alle contacten op de computer een mail met het malware te sturen. Een virus besmet al bestaande software, in vergelijking met een worm die een eigen software is, verder zijn ze zo goed als hetzelfde. Spyware probeert informatie over hoe je je computer gebruikt te achterhalen, bijvoorbeeld welke sites je bezoekt. Adware laat ongewenste reclames zien, vaak monitort het net als spyware hoe je je computer gebruikt om gepersonaliseerde advertenties te laten zien. Ransomware komt je computer in door een trojan horse of een worm, dan versleuteld het bestanden, en moet je geld betalen om weer toegang te krijgen tot die bestanden. Het is echter een slecht idee om geld te betalen omdat je dan criminelen financiert en omdat het helemaal niet zeker is of je je bestanden überhaupt terug krijgt. De aanvallers dreigen ook om al je bestanden te verwijderen als je niet binnen een bepaalde tijd betaalt,

## Aanvallers en verdedigers

verdedigers ontwikkelen steeds betere manieren van beveiliging, aanvallers verzinnen steeds nieuwe manieren om die te doorbreken, zo stopt het gevecht tussen de twee nooit. De aanvallers zijn internetcriminelen. Er zijn goede en slechte hackers, zo worden ethische hackers soms betaalt door een bedrijf om te kijken of hun code veilig is tegen criminelen. diefstal, fraude, afpersing en inbraak (hacken) zijn de meest voorkomende cybercrimes. Diefstal van gegevens gebeurt als iemand jou heeft gehackt, die gestolen gegevens kan de aanvaller gebruiken om zich als jou voor te doen (identiteitsfraude) of dreigen om ze openbaar te maken tenzij jij hem/haar betaalt (afpersing). Bij fraude is iemand je aan het bedriegen om gegevens zoals je IBAN in handen te krijgen. Phishing en soms spyware zijn ook vormen van fraude. Een andere manier van fraude is dat je geld geeft aan iemand (door online daten of een nepshop) en dat je dat geld/een product nooit (terug) krijgt. Afpersing is als iemand geld van je wilt krijgen door te dreigen met iets (bijvoorbeeld je gegevens openbaar maken of deleten). Hierbij maken ze vaak ook gebruik van tijdsdruk. Een bekend voorbeeld is ransomware. Aanvallers die dit doen, halen vaak je e-mailadres uit een gestolen database en sturen dan een e-mail waarin ze beweren dat ze gegevens van je hebben.

Computervredebreuk is een ander woord voor hacken, dit is vaak illegaal en er zijn zelfs specifieke wetten voor. Het hacken dat illegaal is is als je illegaal inbreekt bij websites of computers, ook als je er niks mee doet nadat je hebt ingebroken. Ook een poging doen hiertoe, of hulpmiddelen hiervoor bezitten is strafbaar. Ook is het illegaal om andermans gegevens slecht te bewaren, dat het slecht bewaard is is echter geen reden om het te hacken.

Een andere manier van hacken is ethisch hacken, dit is als een ethische hacker bij bedrijven doorgeeft dat er een beveiligingslek is, soms worden ze daar ook voor betaald. responsible disclosure is als een ethische hacker eerst een lek aangeeft bij degene die daar verantwoordelijk voor is, en als er niets aan wordt gedaan maakt de hacker het openbaar, waardoor de hacker alle eer krijgt en de verantwoordige het snel op moet lossen. Ethisch hacken is technisch gezien wel illegaal, maar meestal wordt er niks aan gedaan omdat ze mensen meer helpen dan lastig vallen. Maar ze moeten niet te ver gaan.

Een zero day is een nog niet ontdekte kwetsbaarheid, daardoor zijn ze belangrijk voor hacken en worden ze soms verkocht voor tienduizenden euro's. Zero days worden verkocht aan criminelen, maar soms ook bedrijven die hun klanten ertegen willen beschermen. Zerodium.com is een site waar je kunt handelen in zero days. Vaak biedt zerodium een stuk meer dan de bedrijven die het echt nodig hebben. Overheden willen zero days hebben om te spioneren of vijandige systemen

te hacken of plat te leggen tijdens bijvoorbeeld een oorlog. De ethische keuze zou zijn om de zero day aan de ontwikkelaars van het systeem door te geven, dan wordt het internet veiliger. Daarom is het verboden voor de overheid om zero days te gebruiken (behalve een paar uitzonderingen). Een extreem voorbeeld is de VS en Israël die zero days gebruikten om Iraanse Kernprogramma's te saboteren. Anonymous is een groep van zogenaamde "hacktivisten" die hacken om censuur tegen te gaan.

# Maatregelen

Veel groepen werken samen om ICT-systemen veilig te houden, namelijk cybersecurity bedrijven, de gebruikers, softwareontwikkelaars en de overheid. Veiligheid vergroten doen zij door: preventie, detectie, repressie en correctie.
Preventie is het voorkomen voordat het gebeurt. Sandboxing laat apps in hun eigen afgesloten ruimte draaien, waar ze alleen toegang krijgen tot hun eigen geheugen en opslag. Voor preventie moet je letten op alle dingen uit het deel **bedreigingen**
Detectie is door hebben wanneer iemand probeert in te breken bij iemands account of de website zelf, daarvoor wordt gebruik van het systeem bijgehouden. Firewalls spelen een grote rol in detectie, zo checkt het voor kwaadaardige gegevens, en of het verkeer van een betrouwbare bron komt, zo beschermt het tegen malware, spam, en hackers. Het beschermt ook tegen DDoS-aanvallen door te controleren of de gebruikers "normaal" bezig zijn. Anti-malware software verwijdert malware door te kijken of bestanden kenmerken van malware bezitten.
Repressie is maatregelen nemen als er een aanval is of als er malware is aangetroffen, correctie is de schade daarvan herstellen. Soms als een website plat ligt door een aanval, kunnen ze switchen naar een back-up systeem, maar de fout moet dan wel zo snel mogelijk gecorrigeerd worden.
Het versleutelen van berichten wordt al heel lang gedaan, Julius Caesar gebruikte een encryptie waarin je elke letter een paar plekjes opschoof in het alfabet, dat was het algoritme symmetrische encryptie. Is encryptie die gebruikmaakt van maar 1 sleutel (de manier waarop je de tekst verandert).
Als je dingen opstuurt naar mensen moet je er voor zorgen dat die andere persoon de sleutel heeft, maar een middel persoon niet. Voor asymmetrische encryptie heb je een publieke sleutel en een geheime sleutel. Met de publieke sleutel wordt een bericht versleuteld. Met de geheime sleutel kan het versleutelde bericht weer worden ontsleuteld. Hierdoor kan iedereen berichten versleutelen, maar niet iedereen ontsleutelen.
Je moet zelf ook dingen doen om veilig(er) te zijn op het internet, als je bijvoorbeeld een oudere computer hebt ben je een makkelijker doelwit. Updates moet je altijd direct downloaden, want als een developer een kwetsbaarheid fixt, is dat alleen op de nieuwste versie. Gebruik altijd vergrendeling op je telefoon, gezichts/vingerafdrukherkenning is het beste. Gebruik sterke en verschillende wachtwoorden en verander ze ook vaak, hiervoor kan je een password manager gebruiken. Maak back-ups van je telefoon en computer, en zorg voor een manier om op een afstand je telefoon/computers gegevens te wissen. Controleer voor beveiligde verbinding en geen vreemde URL, open nooit link uit e-mails. Download alleen apps via vertrouwde fabrikanten, check met een anti-malware programma als je niet zeker bent of je het kan vertrouwen. Link via social media, whatsapp, of e-mail kunnen om phishing gaan of malware bevatten. Klik niet gelijk op OK als een app vraagt voor gegevens. Installeer anti-malware- en anti-adware software en laat deze regelmatig je apparaat checken. Versleutel dingen op een harde schijf of USB-stick. Let op bij zelf geprogrammeerde apparaten (Arduino of Raspberry Pi bijvoorbeeld) aansluiten op het internet, deze zijn kwetsbaar voor hacken. Een VPN kan handig zijn, maar het moet wel een vertrouwbare zijn