

# Security

Informatica subdomein E2. Niet verspreiden.

31 januari 2023

# Inhoudsopgave

<b>1</b>	<b>Digitale veiligheid</b>	<b>3</b>
1.1	Inleiding . . . . .	3
1.2	Vertrouwelijkheid . . . . .	3
1.3	Integriteit . . . . .	6
1.4	Beschikbaarheid . . . . .	8
1.4.1	Encryptie . . . . .	9
1.4.2	DDoS . . . . .	10
1.5	Woordenlijst . . . . .	12
<b>2</b>	<b>Bedreigingen</b>	<b>13</b>
2.1	Inleiding . . . . .	13
2.2	Zwakheden in de architectuur . . . . .	13
2.3	Zwakheden in de communicatie . . . . .	14
2.3.1	Man-in-the-Middle aanval . . . . .	15
2.3.2	HTTPS . . . . .	15
2.3.3	End-to-end encryption . . . . .	16
2.4	Zwakheden bij gebruikers . . . . .	17
2.4.1	Hoe meet je de sterkte van een wachtwoord? . . . . .	18
2.4.2	Password managers . . . . .	18
2.4.3	Populaire wachtwoorden . . . . .	19
2.4.4	Zijn mijn gegevens gehackt? . . . . .	20
2.5	Technieken . . . . .	20
2.5.1	Social engineering . . . . .	20
2.5.2	Phishing . . . . .	21
2.6	Malware . . . . .	22
2.6.1	Trojan Horse . . . . .	22
2.6.2	Worm . . . . .	23
2.6.3	Virus . . . . .	23
2.6.4	Spyware en Adware . . . . .	24
2.6.5	Ransomware . . . . .	24
2.7	Woordenlijst . . . . .	26
<b>3</b>	<b>Aanvallers en verdedigers</b>	<b>28</b>
3.1	Inleiding . . . . .	28
3.2	Computercriminaliteit . . . . .	28
3.2.1	Diefstal . . . . .	28
3.2.2	Fraude . . . . .	28
3.2.3	Afpersing . . . . .	29
3.3	Computervredebreuk . . . . .	29
3.3.1	Na de inbraak . . . . .	30
3.4	Ethisch hacken . . . . .	30
3.4.1	Persvrijheid . . . . .	31
3.5	Spionage en oorlogsvoering . . . . .	31
3.6	Woordenlijst . . . . .	33
<b>4</b>	<b>Maatregelen</b>	<b>34</b>
4.1	Preventie . . . . .	34
4.2	Detectie . . . . .	35
4.3	Repressie en correctie . . . . .	36
4.4	Symmetrische encryptie . . . . .	36
4.5	Asymmetrische encryptie . . . . .	38
4.6	Wat kun je zelf doen? . . . . .	39

4.6.1	Absoluut noodzakelijk . . . . .	39
4.6.2	Verstandig om te doen . . . . .	40
4.7	Woordenlijst . . . . .	41
<b>5</b>	<b>Verdieping: SQL-injecties</b>	<b>42</b>
5.1	Inleiding . . . . .	42
5.2	Wat is een SQL-injectie? . . . . .	43
5.3	Een SQL-query manipuleren . . . . .	45
5.4	De structuur van een database achterhalen . . . . .	48
5.5	SQL-query's uitbreiden . . . . .	49
5.6	Wat is er tegen te doen? . . . . .	51
<b>6</b>	<b>Antwoorden</b>	<b>53</b>
6.1	Digitale veiligheid . . . . .	53
6.2	Bedreigingen . . . . .	54
6.3	Aanvallers en verdedigers . . . . .	56
6.4	Maatregelen . . . . .	56

# 1 Digitale veiligheid

## 1.1 Inleiding

Digitale technologieën veranderen de manier waarop onze maatschappij functioneert. Ook hebben ze invloed op de wijze waarop we ons leven vormgeven. Iedere dag ontstaan er nieuwe mogelijkheden om te werken, te ontspannen en contact met elkaar te hebben. Iedereen gebruikt digitale technologieën op zijn eigen manier. Daarbij worden veel persoonlijke gegevens (eigenschappen) vastgelegd. In feite heeft iedereen zijn eigen digitale identiteit.

Zo zul je waarschijnlijk een digitale identiteit op social media hebben: een Instagram- of Snapchat-account met je naam, waarop je foto's plaatst waar jij en je vrienden op te zien zijn. Maar er zijn meer plekken waar je digitale gegevens achterlaat. Denk aan een account bij een bank of de website waar je je rooster en cijfers kunt bekijken.

Digitale beveiliging is het beveiligen van deze digitale gegevens. Criminelen, hackers, overheden, of zelfs vrienden en familie zijn op zoek naar manieren om achter jouw digitale gegevens te komen. Dit doen ze omdat ze hier (financieel) voordeel van kunnen hebben.

Digitale beveiliging (Engels: digital security) is een overkoepelende term voor alle manieren waarop je eigen digitale identiteit beschermd kan worden.

Iedereen die betrokken is bij het verwerken van digitale gegevens heeft verantwoordelijkheid voor de veiligheid van die gegevens. Zo zullen softwareontwikkelaars zorgen voor een goede beveiliging van een systeem. Jij zelf kunt vaak ook helpen om de veiligheid te vergroten. Bijvoorbeeld door sterke wachtwoorden te gebruiken. En door op je telefoon een wachtwoord of vingerafdruk in te stellen voor ontgrendeling.

Het beveiligen van onze digitale gegevens gaat voornamelijk over de volgende drie aspecten:

1. **Vertrouwelijkheid:** de afscherming van gegevens tegen ongeoorloofde inzage.
2. **Integriteit:** bescherming van gegevens tegen verlies of (on)bedoelde wijzigingen.
3. **Beschikbaarheid:** de mate van storingsvrije toegang tot de gegevens.

### Leerdoelen:

- 1 Je kent de drie beveiligingsaspecten vertrouwelijkheid, integriteit en beschikbaarheid.
- 2 Je kunt verschillende vormen van authenticatie noemen.
- 3 Je weet wat de two factor authentication betekent.
- 4 Je weet het verschil tussen authenticatie, identificatie en verificatie.
- 5 Je bent bekend met encryptie en weet het verschil tussen encryptie en hashing.
- 6 Je weet wat een DDoS-aanval is.

## 1.2 Vertrouwelijkheid

Voordat er toegang is tot persoonlijke gegevens, is er een controle nodig om te kijken of de gebruiker wel toegang mag hebben. Dit proces wordt **authenticatie** genoemd.

Er zijn verschillende vormen van authenticatie. Onder andere door iets dat je **weet** (een wachtwoord of een pincode), iets dat je **hebt** (een sleutel of een pas), of iets dat je **bent** (vingerafdruk of een irispatroon).

**Opdracht 1.** *Bedenk voor elk van de drie genoemde manieren (weet, hebt, bent) nog een derde voorbeeld.*

Behalve de term authenticatie worden ook de termen identificatie en verificatie gebruikt. Bij **identificatie** wordt er aan je gevraagd: “Wie ben je?”. Dat kun je bijvoorbeeld aangeven door het invoeren van een gebruikersnaam/wachtwoord of het laten scannen van je vingerafdruk op je smartphone.

Vervolgens vindt er een **verificatie** plaats. Daarbij gaat het om de vraag: “Ben jij wie je zegt dat je bent?”. Er kan alleen verificatie plaatsvinden als er gegevens van jou bekend zijn. Bijvoorbeeld in een database of in je smartphone. Er kan zo worden gecontroleerd of jij de juiste persoon bent om toegang te krijgen.

**Opdracht 2.** *Als je met het vliegtuig reist, moet je bij de incheckbalie ter controle je ID-kaart of paspoort overhandigen. Bepaal voor deze situatie de identificatie en de verificatie.*

Een veiligere toegangscontrole krijg je door twee vormen van authenticatie met elkaar te combineren. Dit wordt bijvoorbeeld al jarenlang gedaan als je met je pinpas een betaling in de winkel doet. Om die betaling te kunnen doen, heb je iets nodig dat je hebt (je pinpas) en, voor grotere bedragen, ook iets dat je weet (je pincode). Mocht er iemand je pincode weten, dan kan hij zonder pinpas nog niets. En andersom: mocht iemand je pinpas hebben, zonder pincode kan hij geen grote bedragen afrekenen.

Deze combinatie wordt **two factor authentication** genoemd. Op het internet zie je dit bij verschillende websites. Als je dan inlogt met een gebruikersnaam/wachtwoord (iets dat je *weet*), moet je ook nog een *verificatiecode* opvragen op je smartphone (iets dat je *hebt*).

**Bekijk de video op <https://www.youtube.com/watch?v=0mvCeNsTa1g>.**

**Opdracht 3.** *Op social media bestaan ‘verified accounts’. Die worden gebruikt door bekende personen, zodat iedereen kan zien dat de herkomst betrouwbaar is. Op Twitter zie je dan bijvoorbeeld een vinkje in een blauw sterretje staan. Onderzoek hoe je een Twitter-account verified kunt laten maken.*

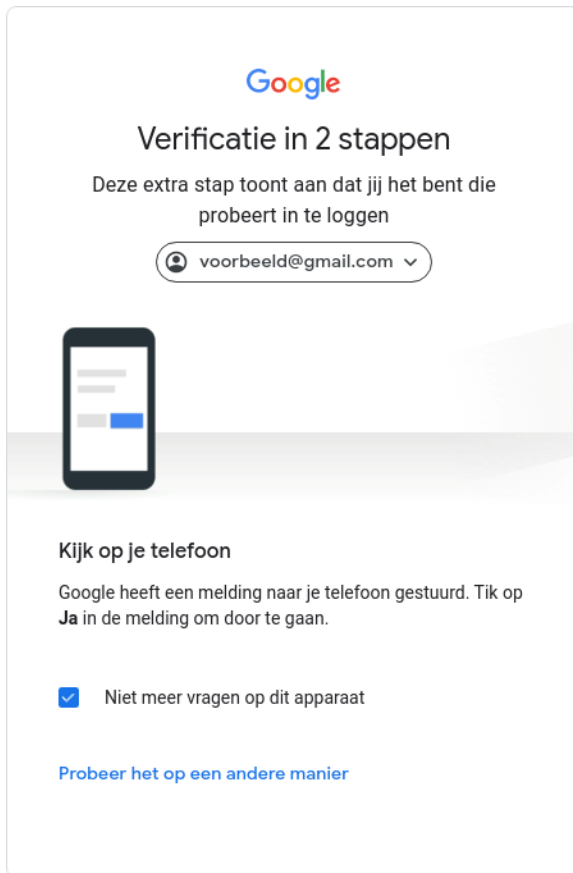
**Opdracht 4.** *Docenten kunnen inloggen op een systeem waar ze cijfers van leerlingen kunnen invoeren.*

- (a) *Waarom is het onveilig als je docent alleen met gebruikersnaam en wachtwoord kan inloggen?*
- (b) *Vraag aan je docent welke vorm van two factor authentication hij of zij moet gebruiken om cijfers in te kunnen voeren. Vind je dat een veilige manier? Leg uit waarom wel of waarom niet?*

**Opdracht 5.** *Als je met het vliegtuig reist, moet je een boarding pass bij je hebben. Op die pass staat een code die wordt gecontroleerd vlak voordat je het vliegtuig binnenstapt. Daarbij moet je ook je ID-kaart of paspoort laten zien.*

*Welke vormen van authenticatie horen bij de volgende handelingen?*

- (a) *Controle boarding pass*
- (b) *Controle BSN-nummer op paspoort of ID-kaart*
- (c) *Vergelijking van foto en lichaamslengte op paspoort of ID-kaart met de passagier*



Figuur 1: Een tweefactorauthenticatie van Google

**Opdracht 6.** *Op school maak je misschien gebruik van een kluisje. Daarvan heb je een sleutel. Je moet ook weten welke kluisje van jou is. Je hebt dus iets dat je weet (je kluisnummer) en iets dat je hebt (je sleutel) nodig om in je kluisje te kunnen. Toch is dat geen echte two factor authentication. Want je klasgenoten weten na verloop van tijd wel waar jouw kluisje ongeveer is. En als iemand je sleutel heeft, kan die met proberen je kluisje vinden en openen.*

*Welke van de volgende extra beveiligingsmaatregelen zorgen ervoor dat er wel sprake is van echte two factor authentication? Antwoord steeds 'ja' of 'nee'.*

- (a) *Op het kluisje ook een vingerafdrukscanner plaatsen.*
- (b) *Op het kluisje ook een touchpad plaatsen waar je een pincode moet invoeren.*
- (c) *Op het kluisje ook een scanner van je schoolpas plaatsen.*
- (d) *Een beveiliging bij de kluisjes plaatsen die je schoolpas controleert op pasfoto of andere gegevens.*

**Opdracht 7.** *Zijn de maatregelen uit vraag 6 wat jou betreft handig? Waarom wel/niet?*

Een techniek die verwant is aan authenticatie, identificatie en verificatie is **screening**. Bij screening worden personen of voertuigen geïdentificeerd. Bijvoorbeeld met camera's. Als een persoon of voertuig op een blacklist staat, wordt hier een melding van gedaan bij de autoriteiten. Die kunnen dan een passende actie ondernemen. Met personen of voertuigen die wel geïdentificeerd

worden, maar niet op een blacklist staan, wordt geen actie ondernomen.

De volgende video is van een Britse journalist, die onderzoekt hoe lang hij onopgemerkt in een Chinese stad kan zijn. **Bekijk de volgende video:** <https://twitter.com/BBCWorld/status/939832896604565505>

### 1.3 Integriteit

Bij jou op school is het alleen voor docenten mogelijk om cijfers in te voeren. Jij als leerling kunt de cijfers alleen bekijken. Het cijfersysteem moet dus controleren of een gebruiker toegang heeft en zo ja, welke **rechten** die gebruiker heeft. De rechten van een gebruiker zijn verbonden aan diens **rol**. Een gebruiker met de rol 'docent' heeft meer rechten dan een gebruiker met de rol 'leerling'. Maar iemand met de rol 'beheerder' heeft nog meer rechten.

De controle of een gebruiker toegang heeft, valt onder vertrouwelijkheid. De controle welke rechten een vertrouwde gebruiker allemaal heeft, noemen we **autorisatie**. We noemen dat ook wel een controle van de **integriteit**.

In het onderdeel C1-2 'Informatie en data' heb je kunnen lezen over de eisen die aan informatie gesteld worden. Hieronder staan ze nogmaals.

Eis	Controlevraag
Volledigheid	Ontbreekt er iets?
Relevantie	Is de informatie afgestemd op het te bereiken doel?
Betrouwbaarheid	Is de informatie correct en afkomstig van een goede bron?
Overzichtelijkheid	Is de informatie goed gestructureerd?
Beschikbaarheid	Is de informatie op het juiste moment beschikbaar?
Doelgerichtheid	Is de informatie gericht op de gebruiker (de doelgroep)?

Met de integriteit van gegevens en informatie bedoelen we dat de kwaliteit van de gegevens zo is, dat er aan al deze eisen wordt voldaan. De gegevens mogen alleen verwerkt worden door gebruikers die hier de juiste rechten voor hebben. Zoals bij het cijfersysteem van jouw school. Door de rechten van de gebruikers af te dwingen, zorgen we ervoor dat de gegevens 'kloppen': er is sprake van integriteit.

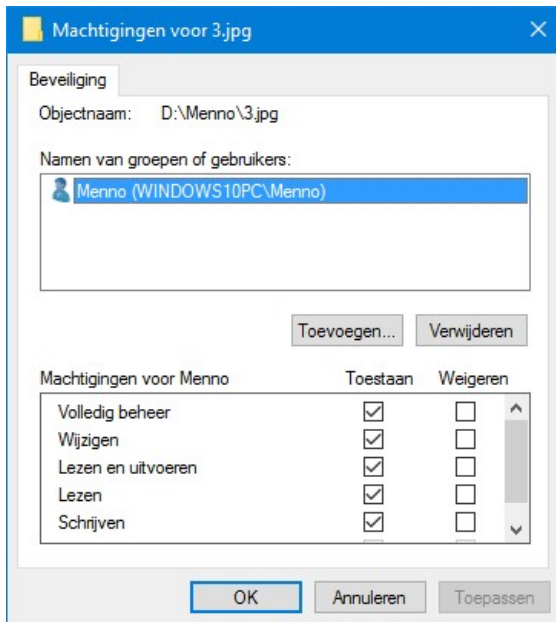
**Opdracht 8.** Bij jou op school wordt er gebruik gemaakt van een ELO (Elektronische Leeromgeving), bijvoorbeeld itslearning, Magister of SOMtoday.

(a) Noem drie verschillende rollen in dit systeem.

(b) Noem per rol een recht.

In de voorbeelden hiervoor heb je gelezen over de integriteit van gegevens in systemen. Maar het begrip integriteit betekent nog meer. In computernetwerken kunnen bepaalde (netwerk)schijven of mappen alleen beschikbaar zijn voor gebruikers met een specifieke rol. Zo heeft de directie van jouw school misschien wel een aparte schijf in het netwerk, waar ze hun bestanden met elkaar kunnen delen. Of kun jij als informaticaleerling bij bestanden, waar leerlingen die geen informatica hebben niet bij kunnen. Om toegang te krijgen tot deze bestanden, hoeft er niet apart ingelogd te worden. Maar er moet wel autorisatie plaatsvinden: de controle of je toegang hebt. Die autorisatie kan door de systeembeheerder worden ingesteld via *file permissions*.

Stel je voor dat je een bestand met iemand anders wilt delen. Bijvoorbeeld via het internet, of via een USB-stick. Hoe weet de ontvanger dan zeker dat het bestand dat hij krijgt het originele bestand is? Misschien is er onderweg wel iets gebeurd met het bestand, waardoor de inhoud is



Figuur 2: Een Windows-menu waarin je machtigingen voor de gebruiker Menno kunt instellen voor het bestand 3.jpg

aangepast. Als dat zo is, dan is de integriteit van het bestand aangetast.

Als je installatiebestanden van programma's downloadt via het internet, zie je er soms een *checksum* bij staan. Bijvoorbeeld bij het FTP-programma FileZilla:

## Download FileZilla Client

The latest stable version of FileZilla Client is 3.34.0

Please select the file appropriate for your platform below.

**Mac OS X**

[FileZilla\\_3.34.0\\_macosx-x86.app.tar.bz2](#) ⓘ

**Size:** 10770370 bytes  
**SHA-512 hash:** 23c9493411226b39a95d9afbeb5fe8c3057643d832afaf50282a4376830d52bf4f25b6fa61f8e49c3e8732652ea99c5b38e9e44dff31107c2e0ac6ef328f920f

Requires OS X 10.9 or newer

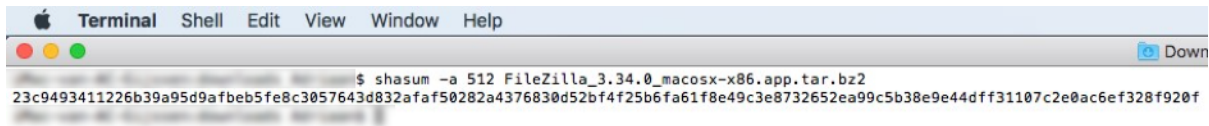
Figuur 3: Onder de download zie je een checksum waarmee je de integriteit van het programma kan controleren.

Deze checksum kun je zien als een *vingerafdruk* van het bestand. Toen de makers van FileZilla het bestand online zetten, hebben ze deze checksum gegenereerd. Als jij het bestand downloadt, en er ook een checksum van genereert, kun je controleren of je exact, tot in de laatste bit, hetzelfde bestand hebt.

**Opdracht 9.** Hieronder staat uitgelegd hoe je op verschillende manieren een checksum genereert:

- In Windows: <https://www.nextofwindows.com/5-ways-to-generate-and-verify-md5-sha-checksum-of-any-file-in-windows-10>
- In macOS: <https://notepad2.blogspot.com/2012/07/mac-os-x-how-to-generate-md5-sha1.html>





```
Terminal Shell Edit View Window Help
$ shasum -a 512 FileZilla_3.34.0_macosx-x86.app.tar.bz2
23c9493411226b39a95d9afbeb5fe8c3057643d832afaf50282a4376830d52bf4f25b6fa61f8e49c3e8732652ea99c5b38e9e44dff31107c2e0ac6ef328f920f
```

Figuur 4: Met de functie shasum kun je in de terminal de checksum genereren. Dat hoort precies dezelfde te zijn als genoemd bij de download in figuur 3.

- Online: <https://md5file.com/calculator>

- (a) Kies een willekeurig bestand, wat is hier de checksum van?
- (b) Deel dit bestand met een klasgenoot en laat hem/haar ook de checksum bepalen. Let op dat jullie beiden eenzelfde soort checksum, zoals MD5 of SHA-512 genereren. Komen ze overeen?

Een andere manier om de integriteit van je data te garanderen, is het maken van back-ups. Mocht er door een onvoorziene oorzaak iets gebeuren met je data, dan is het altijd mogelijk om terug te gaan naar een situatie waarbij de data wel integer was. Meer over back-ups lees je in de volgende paragraaf.

## 1.4 Beschikbaarheid

In de vorige paragrafen heb je gelezen over de vertrouwelijkheid en de integriteit. Je hebt gelezen dat je moet controleren wie er toegang heeft tot je data, en wat er vervolgens met die data mag gebeuren. Een derde aspect is de beschikbaarheid.

De data moet altijd beschikbaar zijn. Dit gaat niet vanzelf. Je zult hiervoor waarschijnlijk af en toe beveiligingsupdates moeten installeren. Of, indien nodig, defecte hardware-onderdelen vervangen.

Mocht het onverhoopt gebeuren dat de data niet (meer) beschikbaar is, moet er een back-up zijn. Een back-up maken kan op verschillende manieren. Bijvoorbeeld via een clouddienst als OneDrive, Google Drive of iCloud Drive. Maar ook op een USB-stick of een externe harde schijf. Bij die laatste twee is het belangrijk om ze niet op dezelfde locatie te bewaren als de data waarvan de back-up is. Stel je voor dat je thuis op een externe harde schijf een back-up hebt staan van je computer, en er breekt een grote brand uit. Dan heb je én je computer niet meer, en de back-up schijf niet meer. Het beste is daarom om een back-up op een fysiek andere plek te bewaren, bijvoorbeeld bij iemand anders thuis.

Bekijk de video op [https://www.youtube.com/watch?v=7A\\_rlttwgvI](https://www.youtube.com/watch?v=7A_rlttwgvI)

**Opdracht 10.** Onderzoek, eventueel samen met je docent, wat het back-up beleid bij jou op school is. Geef hier een korte omschrijving van.

Beveiligingsexperts raden aan om gebruik te maken van het **3-2-1-systeem voor back-ups**: 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. Je kunt bijvoorbeeld je foto's op je computer opslaan, geprinte versies thuis bewaren en een externe harde schijf met alle foto's bij een vriend laten staan.

**Opdracht 11.** Op het Steve Jobscollege in Winsum werkt iedereen met netwerkschijven die door de school worden beheerd. Elke maand maakt de systeembeheerder een kopie van de netwerkschijven op een externe harde schijf die op zijn kantoor staat.

*Welk advies zou je deze school geven met betrekking tot back-ups?*

#### 1.4.1 Encryptie

Voor een toegangscontrole moeten er ook gegevens worden opgeslagen. Maar het opslaan (en verzenden) van wachtwoorden, pincodes, vingerafdrukken en dergelijke gegevens brengt ook uitdagingen met zich mee. Stel je voor dat het hackers lukt om een database met wachtwoorden in te zien. Het is dan ineens erg eenvoudig geworden om toegang te krijgen tot persoonlijke gegevens. De impact voor gebruikers is dan groot. Een wachtwoord kun je nog wijzigen, maar een vingerafdruk niet.

Niet alleen wachtwoorden of vingerafdrukken moeten zorgvuldig worden opgeslagen. Je hebt misschien wel een USB-stick waarop bestanden staan, waarvan je niet wilt dat iedereen die kan zien. Of bestanden op je computer, die alleen jij mag bekijken.

Gevoelige bestanden kunnen versleuteld worden opgeslagen en/of verzonden. Hiervoor wordt er gebruikgemaakt van **encryptie**. Door middel van een sleutel, bijvoorbeeld een wachtwoord, kan de inhoud van een bestand wiskundig worden 'gehusseld'. Met dit nieuwe bestand kun je niets; je moet de inhoud eerst weer op een correcte manier terugzetten. Dat kan alleen met de sleutel. Die moet dus geheim blijven!

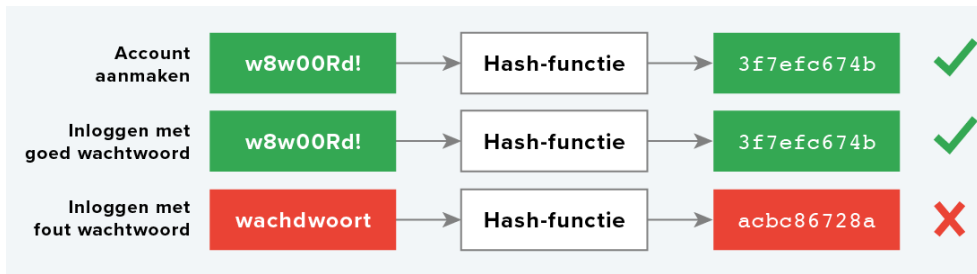
Encryptie wordt niet alleen gebruikt om bestanden te beveiligen, maar ook om communicatie geheim te houden. Je ziet dat wanneer je in WhatsApp een nieuw gesprek met iemand begint: *Berichten en oproepen worden end-to-end versleuteld. Niemand buiten deze chat kan ze lezen of beluisteren.* WhatsApp husselt dus alle berichten die je verstuurt. Zo kan niemand meelesen, behalve de persoon aan wie je de berichten verstuurt.



Figuur 5: Een bericht van WhatsApp over het gebruik van end-to-end-encryptie

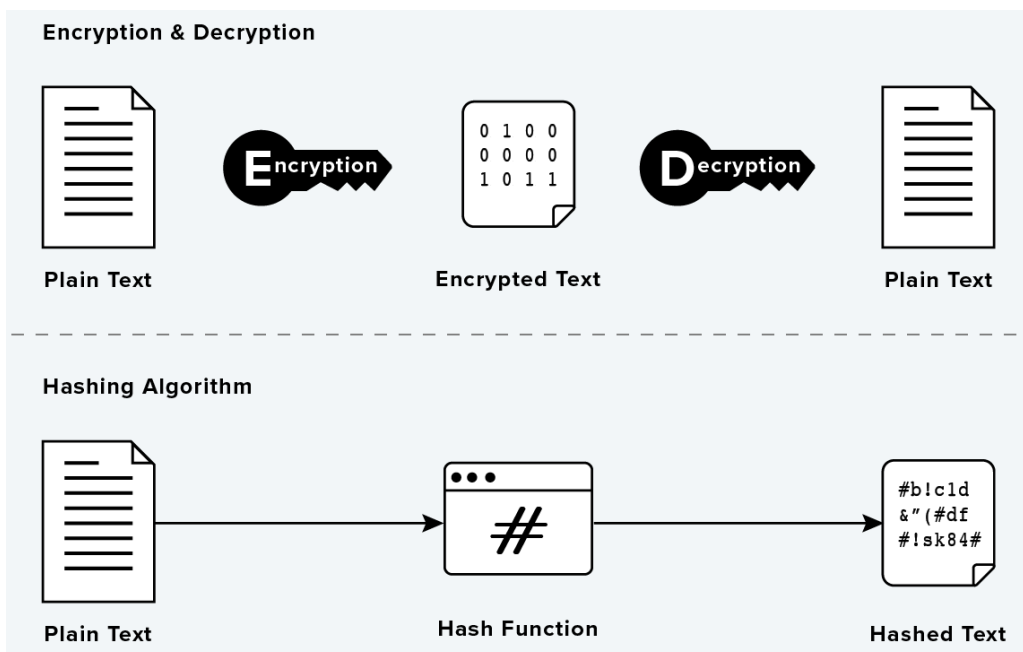
Voor het opslaan van wachtwoorden, vingerafdrukken en dergelijke wordt gebruikgemaakt van **hashing**. Hiermee wordt bijvoorbeeld het wachtwoord, net als bij encryptie, gehusseld. Bij hashing kun je echter niet meer terug naar het origineel. Heeft een kwaadwillende dus een database met gehashte wachtwoorden gestolen, dan kan hij nog steeds de originele wachtwoorden niet verkrijgen. Via de site <https://sha512.online> kun je met het SHA512 algoritme een hash genereren bij een door jij ingevoerde tekst. Probeer het maar eens uit.

Hoe weet een website dan dat je het juiste wachtwoord invoert wanneer je probeert in te loggen? Dat gebeurt door je wachtwoord nogmaals te hashen. Wanneer je inlogt, wordt er van het wachtwoord dat je opgeeft een hash gemaakt. Die hash wordt vergeleken met de hash in de database. Zijn de hashes gelijk aan elkaar, dan waren de wachtwoorden ook gelijk aan elkaar en mag je verder. Na het hashen wordt er dus niets met het oorspronkelijke wachtwoord gedaan.



Figuur 6: Het gehashte wachtwoord wordt opgeslagen bij het aanmaken van een account. Bij het inloggen wordt de gehashte input vergeleken met het gehashte opgeslagen wachtwoord.

Vingerafdrukken worden op smartphones in een apart deel van de hardware opgeslagen, waartoe andere processen geen toegang hebben. Leg je je vinger op de scanner, dan wordt aan dat aparte deel gevraagd of het een bekende vinger is. De apps krijgen je vingerafdruk nooit te zien.



Figuur 7: Encryptie/decryptie en hashing

Bekijk deze video over hoe veilig hashing is: [https://www.youtube.com/watch?v=S9JGmA5\\_unY](https://www.youtube.com/watch?v=S9JGmA5_unY).

#### 1.4.2 DDoS

Je webmail, de website van je bank en de OV-planner moeten zo veel als mogelijk beschikbaar zijn. Het komt toch wel eens voor dat websites of andere digitale diensten tijdelijk niet beschikbaar zijn. Dit kan te maken hebben met een zogenoemde DDoS-aanval. De afkorting DDoS staat voor Distributed Denial Of Service. Oftewel, een gecontroleerde aanval om een service (tijdelijk) uit te schakelen.

Stel je voor dat de website van jouw school gemiddeld 100 aanvragen per minuut krijgt. Dit zullen vooral leerlingen zijn die hun rooster en/of huiswerk bekijken. Bij een DDoS-aanval worden er

vele duizenden aanvragen per seconde gedaan. Een website kan dit niet allemaal verwerken en zal daardoor crashen.

Technisch is het niet heel moeilijk om een DDoS-aanval uit te voeren. Er zijn op het internet verschillende ‘aanbieders’ te vinden, waar je tegen een betaling een DDoS-aanval kunt aanvragen. Maar wees ervan bewust dat de straffen op het uitvoeren van een DDoS-aanval hoog zijn.

Een DDoS-aanval is strafbaar, omdat deze vaak grote gevolgen heeft. Wordt een ziekenhuis bijvoorbeeld aangevallen, waardoor belangrijke apparatuur niet meer werkt, dan lopen de patiënten gevaar. En als een bank onbereikbaar wordt door een DDoS-aanval, kunnen de rekeninghouders niet meer bij hun geld.

### Zo werkt een DDoS-aanval



Figuur 8: Schematisch overzicht van een DDoS-aanval

Er zijn verschillende mogelijkheden om een DDoS-aanval tegen te gaan. Een veel gebruikte manier is om het verkeer richting een website te filteren. Alleen goedgekeurd verkeer zal worden doorgelaten. Mocht blijken dat er grote hoeveelheden ongewenst verkeer zijn, kan er worden gekozen om het internetverkeer om te leiden naar een gespecialiseerde anti-DDoS-dienst. Zo'n dienst wordt ook wel een 'Anti-DDoS wasstraat' genoemd. Die heeft verschillende geavanceerde methoden om te controleren of het verkeer ongewenst is. Zo blijft alleen het verkeer over dat legitiem is.

**Opdracht 12.** Zoek op het internet naar een recent nieuwsbericht over een DDoS-aanval. Beantwoord de volgende vragen:

- Welk nieuwsbericht heb je gevonden?
- Waarop was de DDoS-aanval gericht?
- Is er iets bekend over de aanvallers?
- Is er schade aangericht?

## 1.5 Woordenlijst

De volgende belangrijke termen kwamen voor in hoofdstuk 1.

- vertrouwelijkheid - afscherming van gegevens tegen ongeoorloofde inzage.
- integriteit - bescherming van gegevens tegen verlies of (on)bedoelde wijzigingen.
- beschikbaarheid - de mate van storingsvrije toegang tot de gegevens.
- authenticatie - controle of de gebruiker wel toegang mag hebben.
- identificatie - een gebruiker geeft aan wie hij is (bijvoorbeeld met gebruikersnaam/wachtwoord of een vingerafdruk).
- verificatie - er wordt gecontroleerd dat de gebruiker inderdaad is wie hij zegt dat hij is.
- two factor authentication - er worden twee vormen van authenticatie gecombineerd (twee van: wie je bent, wat je weet en wat je hebt).
- screening - personen of voertuigen worden preventief geïdentificeerd en vergeleken met een blacklist.
- autorisatie - controle welke rechten een gebruiker heeft / controle van de integriteit.
- file permissions - instellingen welke gebruiker welke rechten heeft voor bestanden op een systeem.
- checksum - hashcode gegenereerd door een volledig programma, wordt gegeven bij een download en is lokaal te controleren in de command line.
- 3-2-1-systeem voor backups - er moeten drie kopieën van data zijn, op minimaal twee manieren opgeslagen, waarvan één op een andere locatie.
- encryptie - versleuteling die omkeerbaar is. (Het omgekeerde heet decryptie).
- end-to-end encryptie - alleen de zender en de ontvanger van een bericht kunnen het bericht lezen.
- hashing - genereren van een (hash)code op basis van data. Dit is onomkeerbaar, dus je kunt niet de originele data terughalen op basis van de hashcode.
- DDoS-aanval (distributed denial of service) - een aanval waarbij heel veel computers tegelijk een opdracht aan een (web)server geven. De server wordt daardoor te zwaar belast en kan uitvallen.

## 2 Bedreigingen

### 2.1 Inleiding

Onze digitale veiligheid wordt op allerlei manieren bedreigd. Aanvallers maken gebruik van verschillende zwakheden om toegang te krijgen tot onze digitale gegevens. In dit hoofdstuk bekijken we de volgende zwakheden:

- Zwakheden in de architectuur.
- Zwakheden in communicatie.
- Zwakheden bij gebruikers.

Ook bekijken we welke technieken worden ingezet om misbruik te maken van deze zwakheden. Wie er achter deze bedreigingen kunnen zitten, lees je in hoofdstuk 3. Wat je tegen al deze bedreigingen kunt doen, lees je in hoofdstuk 4.

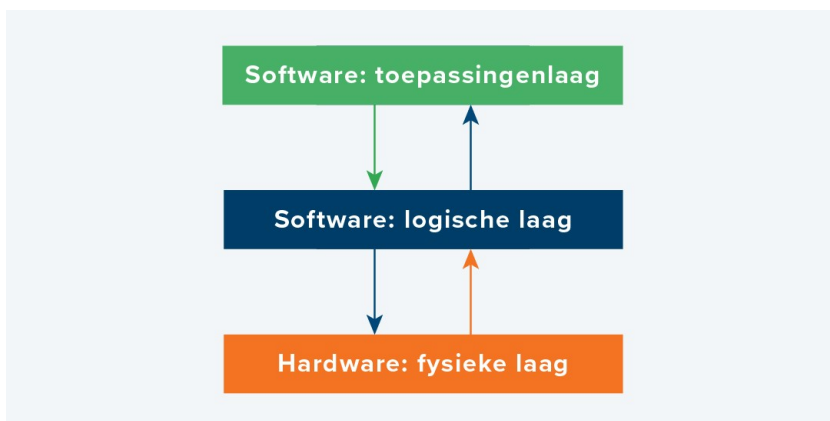
#### Leerdoelen:

- 1 Je kunt zwakheden in de architectuur, de communicatie en bij gebruikers benoemen..
- 2 Je weet wat een SSL-certificaat is.
- 3 Je bent bekend met de technieken social engineering en phishing.
- 4 Je kunt verschillende vormen van malware benoemen en aangeven wat overeenkomsten en verschillen zijn.

### 2.2 Zwakheden in de architectuur

In het onderdeel E1 heb je gelezen dat je in ICT-producten vaak drie lagen kunt onderscheiden:

1. Fysieke laag;
2. Logische laag;
3. Toepassingenlaag.



Figuur 9: Het drielagenmodel

Een zwakheid in de architectuur maakt gebruik van een tekortkoming in een van deze lagen, of in de communicatie tussen twee lagen. Er is dan een fout gemaakt in het ontwerp van de laag of

de communicatie. Vaak had de ontwerper of maker die fout helemaal niet voorzien.

Een voorbeeld is de camera op je telefoon. Wanneer een app gebruik wil maken van je camera, verschijnt er eerst een pop-up waarin je toestemming moet geven. Het kan gebeuren dat er een manier wordt gevonden om de camera te gebruiken zonder dat de pop-up verschijnt. Een aanvaller kan dan meekijken met je camera zonder dat je dat doorhebt.

In het nieuws wordt vaak gesproken over een lek in een website of app. Een kwaadwillende partij heeft dan een zwakte in de architectuur gevonden en maakt daarvan gebruik om schade aan te richten.

Een ander voorbeeld is de vraagtaal SQL. Daarover hebben we geleerd in het onderdeel Databases. Een app of website kan gegevens ophalen uit een database en deze weergeven. Stel dat het lukt om de vraag vanuit de app naar de database aan te passen. Dan is het ineens mogelijk om andere gegevens uit de database te selecteren dan die oorspronkelijk worden gevraagd. En het is in theorie zelfs mogelijk om nieuwe gegevens toe te voegen, bestaande gegevens aan te passen en zelfs te verwijderen!



Figuur 10: Een geslaagde aanval door middel van SQL-injectie

Deze techniek wordt een **SQL-injectie** genoemd. Het is een vorm van hacken waardoor er gegevens in een slecht beveiligde databaseverbinding kunnen worden aangepast.

Als je een app of programma maakt dat een database gebruikt, moet je altijd zorgen dat deze verbinding goed beveiligd is en dat je input van gebruikers altijd filtert.

Meer over SQL-injecties kun je lezen in hoofdstuk 5.

**Bekijk de volgende video met een voorbeeld van een SQL-injectie:**  
[https://www.youtube.com/watch?v=WWJTsKaJT\\_g](https://www.youtube.com/watch?v=WWJTsKaJT_g).

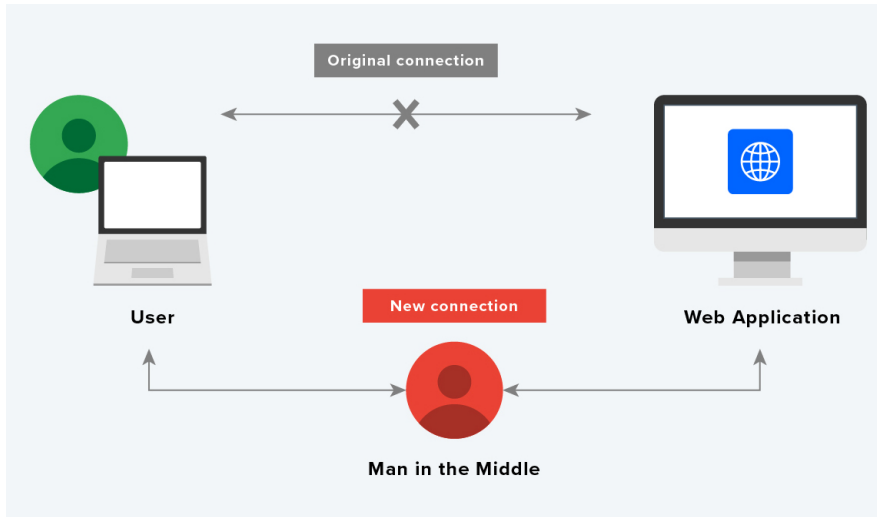
Zwakheden in de architectuur kun je verhelpen door ze zelf op te sporen en op te lossen, voordat iemand met kwade bedoelingen ze heeft gevonden. Dat doe je door de architectuur te **testen**. Je gaat dan zelf proberen om de architectuur aan te vallen. Dit werk wordt vaak verricht door ethische hackers. Hierover lees je meer in hoofdstuk 3.

## 2.3 Zwakheden in de communicatie

Verschillende apparaten zijn met elkaar verbonden. Bijvoorbeeld door middel van internet. Hierdoor kunnen ze met elkaar communiceren. Maar die communicatie moet wel op een veilige manier gebeuren. Als jij op je telefoon een wachtwoord intypt op een website, wordt dit wachtwoord verzonden vanaf je telefoon naar de website. Het ingevoerde wachtwoord mag voor niemand zichtbaar zijn, behalve voor de website waarop je inlogt.

### 2.3.1 Man-in-the-Middle aanval

Met een man-in-the-middle aanval kan de verbinding tussen twee apparaten afgeluisterd worden. Stel dat een gebruiker gegevens invult op een website. Die gegevens worden, als het goed is, direct naar de website verzonden. Maar als er *iemand* tussen deze verbinding komt, en de binnenkomende gegevens van de gebruiker direct doorstuurt naar de website, heb je niet door dat je afgeluisterd wordt.



Figuur 11: Een schematische weergave van een man-in-the-middle aanval

Deze techniek wordt nog al eens gebruikt door een openbaar wifi-netwerk op te zetten. Nietsvermoedende gebruikers verbinden hiermee en maken gebruik van het internet. Maar ondertussen loopt al het internetverkeer via de hotspot van de aanvaller.

In hoofdstuk 4 lees je tips over hoe je moet omgaan met openbare wifi-hotspots. Kijk ook deze video daarover: <https://www.youtube.com/watch?v=HEBQn8x44JM>.

### 2.3.2 HTTPS

In de protocollen HTTP en HTTPS staat onder andere beschreven hoe het internetverkeer geregeld is. De S van HTTPS staat voor secure. Hiermee kan er een beveiligde verbinding worden opgezet tussen een client en een server. Het blijft dan mogelijk om internetverkeer af te luisteren, maar het is niet meer in te zien, omdat het door middel van encryptie beveiligd is. De techniek die hier achter zit, is asymmetrische encryptie. Hierover lees je meer in paragraaf 4.6.

Als je gebruikmaakt van HTTPS-verbindingen, ben je ook een stuk minder vatbaar voor een man-in-the-middle aanval, omdat de verstuurde gegevens versleuteld zijn.

Om HTTPS mogelijk te maken, moet de beheerder van een website een SSL-certificaat installeren. Dat certificaat bevat gegevens over degene van wie de website is. Op die manier weet de client wie er achter de server zit waarmee hij verbonden is. Omgekeerd is dat niet het geval. Als client hoef je geen certificaat te hebben. Dat betekent dat de server niet weet wie de gebruiker is die de website bezoekt. Als de server per se moet weten wie de client is, zal de website aan de gebruiker moeten vragen om in te loggen.

Het certificaat moet door de beheerder van de website worden aangevraagd bij een centrale organisatie. Die organisatie geeft alleen certificaten uit aan mensen, instanties of bedrijven die



bewezen hebben dat de website ook echt van hen is, bijvoorbeeld door ze een stukje code op de website te laten publiceren. Een webbrowser vertrouwt alleen certificaten die door zulke organisaties zijn uitgegeven. Dat laat hij zien met een hangslotje in de adresbalk.

**Opdracht 1.** *Let's Encrypt is een populaire instantie die certificaten voor HTTPS uit geeft, omdat Let's Encrypt dat als enige partij gratis doet. Bekijk de pagina met uitleg <https://letsencrypt.org/docs/challenge-types/>. Op welke manieren kun je bewijzen dat een website van jou is? Antwoord steeds 'ja' of 'nee'.*

- (a) Door een bestand op je website te zetten.
- (b) Door een brief naar Let's Encrypt te sturen.
- (c) Door een DNS-record aan te maken.

**Opdracht 2.** *Bezoek een website van de Nederlandse overheid, bijvoorbeeld <https://rijksoverheid.nl/>. Bekijk de details van het HTTPS-certificaat. In Chrome doe je dit door op het slotje te klikken, waarna je op 'Certificaat' klikt. In Firefox klik je op het slotje, dan op het pijltje en vervolgens op 'Meer informatie'. In Edge klik je op het slotje, dan op 'Verbinding is veilig' en ten slotte op het certificaat-icoontje rechtsboven.*

- (a) Door wie is het certificaat uitgegeven? Sommige webbrowsers noemen het niet 'uitgeven', maar verlenen of verifiëren.
- (b) Bekijk de lijst van vertrouwde certificaat-organisaties op <https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport>. Vind je de organisatie uit vraag a hierin terug?

### 2.3.3 End-to-end encryption

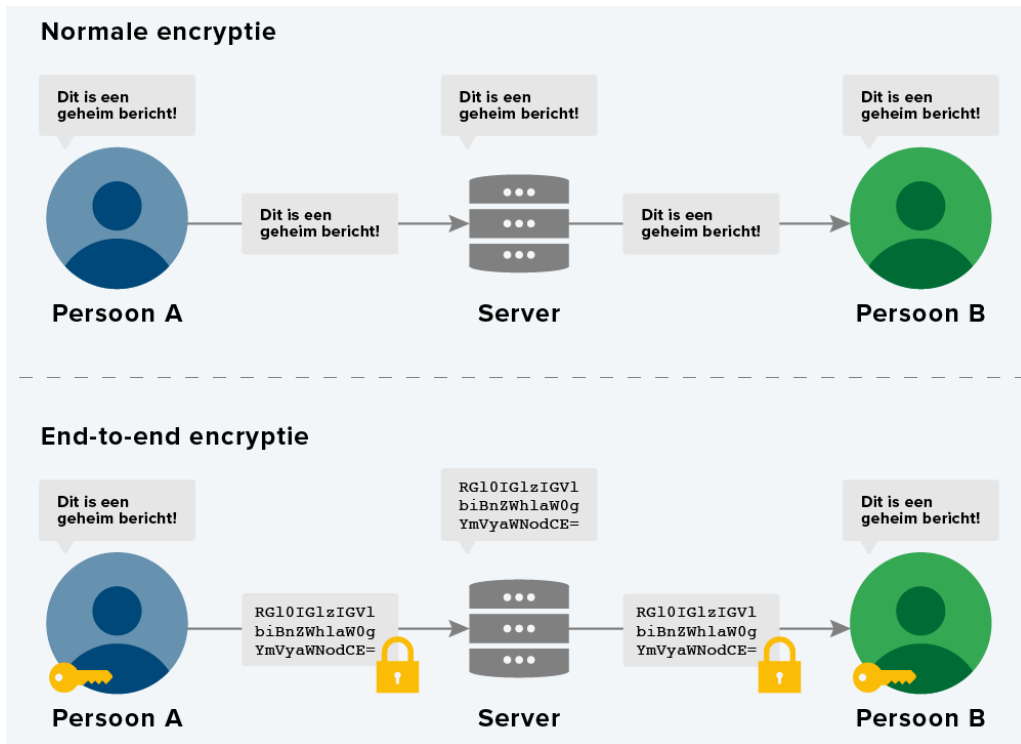
Door middel van een HTTPS-verbinding worden de verzonden gegevens door middel van encryptie onleesbaar gemaakt. Waar een HTTPS-verbinding alleen zorgt voor de beveiliging tussen de client en een server, gaat **end-to-end encryption** nog een stap verder.

Bij een HTTPS-verbinding worden de gegevens versleuteld verstuurd tussen de client en de server. De server kan dus de oorspronkelijke, onversleutelde gegevens inzien en opslaan. Aanvallers maken maar hiervan al te graag gebruik door bijvoorbeeld op servers in te breken en de onversleutelde gegevens te stelen.

End-to-end encryption versleutelt de gegevens nog voordat ze het internet op gaan, en ontsleutelt ze pas wanneer ze het internet verlaten. Alleen jij en de ontvanger kunnen ze ontsleutelen. Krijgt een hacker toegang tot de server, dan zal hij nooit de onversleutelde gegevens in kunnen zien. End-to-end encryption lost dus problemen als gevolg van zwakheden in de communicatie én zwakheden in de architectuur op!

**Opdracht 3.** *Bekijk deze pagina met uitleg over beveiliging van WhatsApp-berichten: <https://www.whatsapp.com/security?lg=en&lc=NL>. Hoe worden WhatsApp-berichten beveiligd? Kies uit:*

- A. De gebruikers zijn zelf verantwoordelijk voor de versleuteling.
- B. Berichten zijn versleuteld met een uniform slot, dat door WhatsApp speciaal is ontwikkeld en voor alle berichten gebruikt wordt.
- C. Berichten zijn versleuteld met een slot, en alleen de ontvanger en jij hebben de sleutel om het bericht te ontsleutelen.
- D. Berichten zijn versleuteld met een slot, en alleen de ontvanger, jij en WhatsApp zelf hebben de sleutel om het bericht te ontsleutelen.



Figuur 12: Normale encryptie vs. end-to-end encryptie

## 2.4 Zwakheden bij gebruikers

Niet alleen bij de systemen die we gebruiken zitten zwakheden, maar ook bij ons zelf. Misschien zijn wij mensen wel de zwakste schakel in het geheel.

Een van de bekendste voorbeelden van zwakheden bij gebruikers is de manier waarop wij met wachtwoorden omgaan. Voor veel diensten op het internet moet je een gebruikersnaam en wachtwoord gebruiken. Vaak kiezen mensen voor simpele wachtwoorden die makkelijk te onthouden zijn, zoals Welkom123 of gewoon hun voornaam. Helaas zijn die wachtwoorden makkelijk te kraken: een aanvaller kan er makkelijk achter komen en inbreken op je account.

Wat bedoelen we met het kraken van wachtwoorden? Een aanvaller probeert dan elk mogelijk wachtwoord om in te loggen op je account, totdat het juiste wachtwoord is gevonden. Speciale programma's zijn in staat om duizenden wachtwoorden per seconde te proberen. Deze techniek heet **brute force**: er wordt brute kracht ingezet om het wachtwoord te ontdekken.

Veel websites voorkomen een brute force aanval door een grens te stellen aan het aantal malen dat een wachtwoord geprobeerd mag worden. Dat is helaas niet voldoende: bij een zwakheid in de architectuur kan het alsnog gebeuren dat aanvallers duizenden pogingen kunnen doen.

Om te voorkomen dat je wachtwoord bij een brute force aanval gekraakt kan worden, is het belangrijk om het wachtwoord zo ingewikkeld mogelijk te maken. Veel websites helpen je hierbij door het gebruik van cijfers en speciale tekens te verplichten. Dankzij die extra tekens zijn er meer mogelijke wachtwoorden, waardoor een aanvaller veel meer pogingen moet doen.

- Hoe meer tekens, hoe veiliger. Bij een lang wachtwoord is het al snel niet meer de moeite waard om er een brute force aanval op los te laten.

- Hoe meer soorten tekens, hoe veiliger. Hoe complexer het wachtwoord, hoe meer mogelijkheden een hacker moet inzetten om het ingewikkelde wachtwoord te vinden.
- Gebruik geen voor de hand liggende woorden, zoals woorden in een woordenboek, de naam van de website of je eigen naam of geboortedatum.
- Gebruik voor iedere website of dienst een ander wachtwoord.
- Pas je wachtwoorden minimaal één keer per jaar aan.

Een overzicht van de beste passwordmanagers vind je hier: <https://www.pcmag.com/picks/the-best-password-managers>.

Sommige diensten bieden de mogelijkheid een geheime vraag te gebruiken. Als je je wachtwoord niet meer weet, kun je die vraag beantwoorden om toch bij je gegevens te komen. Deze mogelijkheid moet je niet gebruiken. Veel van deze vragen zijn voor criminelen eenvoudig te beantwoorden, door naar je sociale profielen op Facebook of Instagram te kijken!

#### 2.4.1 Hoe meet je de sterkte van een wachtwoord?

Is jouw wachtwoord sterk genoeg? Veel websites meten de sterkte van je wachtwoord aan de hand van bepaalde eisen. Je moet bijvoorbeeld genoeg speciale tekens gebruiken, je gebruikersnaam mag er niet in zitten of je moet het niet eerder hebben gebruikt. Echt waterdicht is zo'n manier van meten niet. We kijken naar drie manieren om de wachtwoordsterkte te meten:

- In 1948 ontwikkelde Claude Shannon, een bekend wiskundige, een formule om de **entropie** van informatie op te meten. Je meet dan de willekeurigheid van bepaalde informatie. Dat is een goede manier om de wachtwoordsterkte te meten. Immers, hoe willekeuriger het wachtwoord, hoe moeilijker je het kunt raden!
- Een andere manier die vaak wordt toegepast, is om te kijken hoeveel wachtwoorden lijken op jouw wachtwoord. Er zijn maar  $10^5$  (100.000) wachtwoorden van 5 cijfers, maar wel  $26^5$  (11.881.376) wachtwoorden van 5 letters. Zijn er meer wachtwoorden die op jouw wachtwoord lijken, dan is je wachtwoord unieker en dus sterker.
- Ongeveer 10 jaar geleden was een medewerker van Dropbox de wachtwoordsterktemeters op websites zat. Ze werkten (toen) nooit goed en gaven verkeerde aanbevelingen. Daarom ontwikkelde hij in 2012 **zxcvbn**. Door het wachtwoord slim te analyseren, kan zxcvbn allemaal patronen ontdekken en op die manier bepalen hoe sterk je wachtwoord is. Het is ook het enige algoritme dat controleert of je wachtwoord bekende woorden bevat.

#### 2.4.2 Password managers

Voor iedere website een ander wachtwoord van minimaal 12 tekens zelf onthouden, is bijna niet te doen. Maak daarom gebruik van een passwordmanager. Dat is software die al je wachtwoorden veilig bewaart. Je hoeft zelf maar één wachtwoord te onthouden. Dat moet natuurlijk wel een moeilijk te raden wachtwoord zijn. De passwordmanager installeer je bijvoorbeeld op je smartphone en als add-on in je webbrowser.

Als je bent ingelogd bij de passwordmanager, vult deze automatisch de juiste gebruikersnaam en wachtwoord in als je wilt inloggen op een website. Die gegevens hoeft je dus niet zelf te onthouden. Als je ergens een nieuw account aanmaakt, kun je de passwordmanager een heel sterk wachtwoord laten kiezen. Je kunt ook iemand die je helemaal vertrouwt toegang geven tot je passwordmanager. Zo zorg je ervoor dat je bij je gegevens kunt, ook als je het wachtwoord van de passwordmanager zelf vergeet.

Hoe veilig het ontgrendelen van je smartphone is, zie je in de volgende video:  
<https://www.youtube.com/watch?v=WX4AswCzwug>.

**Opdracht 4.** Bekijk de volgende lijst met wachtwoorden. Geef aan of ze goed of slecht zijn.

- (a) 1234567890
- (b) passw0rd
- (c) faceb00k\_Jan
- (d) iCfbqyfe01Gyhee5
- (e) tfkubmwe
- (f) C@ts-and\_Dogs-L!ving-t0g3ther

### 2.4.3 Populaire wachtwoorden

Regelmatig worden er door nieuwswebsites en andere media lijsten uitgebracht van de meest gebruikte wachtwoorden. Deze lijsten worden gebaseerd op openbaar gemaakte hacks. Wat opvalt is dat er al jarenlang eenvoudige wachtwoorden in de top-50 en zelfs in de top-5 staan.



Figuur 13: De 50 meest gebruikte wachtwoorden

**Opdracht 5.** Op Wikipedia staat een lijst van meestgebruikte wachtwoorden over de jaren heen. Bekijk die lijst op [https://en.wikipedia.org/wiki/List\\_of\\_the\\_most\\_common\\_passwords](https://en.wikipedia.org/wiki/List_of_the_most_common_passwords). Noem enkele wachtwoorden die ieder jaar in de top-25 voorkomen.

#### 2.4.4 Zijn mijn gegevens gehackt?

Regelmatig duiken er op internet lijsten op van wachtwoorden. Die zijn afkomstig van systemen die gehackt zijn. Hackers maken deze lijsten openbaar om het bewustzijn van mensen te vergroten en ze te dwingen om hun wachtwoorden aan te passen. Een website waar je veel van deze wachtwoorden kunt vinden is: <https://haveibeenpwned.com/>.

Hackers bieden de gestolen gegevens soms ook te koop aan. Zo belanden onze gegevens, zoals e-mailadressen, telefoonnummers en wachtwoorden, bij kwaadwillende partijen. Ze gebruiken die om doelgericht nepmails te sturen. Daarmee kunnen ze je manipuleren om nog meer gegevens prijs te geven. Meer hierover vind je in de volgende paragraaf. Ook lees je over andere technieken die worden ingezet om misbruik te maken van zwakheden bij gebruikers.

**Bekijk deze video over databreaches:** <https://www.youtube.com/watch?v=dWVzU37eO-s>.

## 2.5 Technieken

Criminelen maken gebruik van verschillende technieken om achter onze persoonlijke gegevens te komen. Vaak worden er verschillende technieken gecombineerd om het doel te bereiken. We bespreken drie veelgebruikte technieken:

- Social engineering;
- Phishing;
- Malware.

Malware is onder te verdelen in verschillende soorten. Deze soorten komen aan de orde in paragraaf 2.6.

### 2.5.1 Social engineering

Social engineering is geen digitale techniek. Het is meer een methode die aanvallers gebruiken om mensen te bewerken. Hoe sterk een digitale beveiliging ook is, een mens blijft altijd een van de zwakste schakels. Social engineering maakt gebruik van psychologische trucjes om mensen iets te laten doen wat ze eigenlijk niet willen doen, zoals het vrijgeven van gegevens of wachtwoorden. Dat doen social engineers vaak door zich voor te doen als iemand anders, zoals een medewerker van het bedrijf of de bank van het slachtoffer.

Er zijn verschillende aanvalstechnieken. Zo kunnen slachtoffers onder andere via een telefoongesprek of via e-mail benaderd worden. In de meeste gevallen zijn de aanvallen goed voorbereid en is het lastig om ze door te hebben. Als je in een bedrijf van meer dan 1000 medewerkers werkt, ken je niet iedereen bij naam. Als je dan een telefoontje krijgt van 'Nick van de IT-afdeling' weet je niet eens of Nick daar inderdaad werkt.

In telefoongesprekken en e-mails kunnen hackers allerlei 'psychologische trucs' uithalen, om hun doel te bereiken. Twee mooie voorbeelden hiervan staan hieronder.

**Bekijk deze video voor het eerste voorbeeld:** <https://www.youtube.com/watch?v=F78UdORII-Q>.

Het tweede voorbeeld:

*Er zijn bedrijven die op afspraak controleren hoe vatbaar andere bedrijven zijn voor social engineering. Op deze website: <https://www.compact.nl/articles/social-engineering-de-kunst-van-het-misleiden/> vind je*

er een aantal voorbeelden van. Een van de voorbeelden die daar genoemd wordt, staat hieronder.

*"We zijn wel eens verkleed als Sinterklaas en Zwarte Piet een zwaarbeveiligd datacentrum binnengedrongen. Het datacentrum lag op een afgezonderde locatie en was omgeven door metershoge hekken met prikkeldraad, tientallen camera's en een aarden wal die het zicht op het gebouw ontnam. Een week van tevoren hadden we de beveiliging al aan de telefoon gehad en ons voorgedaan als HR-medewerkers die belden in verband met de aankomende Sinterklaasactiviteiten op de verschillende locaties. De beveiliging had dus al 'iets' van de activiteiten gehoord, maar werd toch overrompeld door de situatie. Om op het terrein te komen, moest eerst een soort 'checkpoint Charlie' worden gepasseerd waar een beveiligingsmedewerker achter kogelvast glas met de beveiliging binnen overlegde over de te nemen stappen. Min of meer tot onze eigen verbazing werden we doorgelaten het terrein op, terwijl de deur achter ons weer vergrendeld werd. Bij het datacentrum zelf aangekomen, liepen we ook weer direct tegen een glazen beveiligingsruimte aan waar zich een vijftal beveiligingsmedewerkers bevond. Eén blik in onze zware zak met kilo's pepernoten was voldoende geweest om de opnameapparatuur van de spionagecamera te ontdekken en ons te ontmaskeren. 'Hallo! Hier zijn we dan!', riepen we, en vulden het bakje waar normaliter de paspoorten onder het glas worden doorgeschoven met pepernoten. Nadat we één van de beveiligers nog hadden omgekocht met een chocoladeletter hebben we een rondje door het pand gemaakt en zijn we zonder problemen weer vertrokken."*

## 2.5.2 Phishing

Phishing is een techniek die door criminelen gebruikt wordt in combinatie met social engineering. Met phishing worden slachtoffers, veelal via een e-mail, naar een valse website gelokt. Die e-mail en website zijn vaak nauwkeurig nagemaakt. Veelal gaat het om e-mails van banken, waarin staat dat er iets mis is met je rekening. Om het op te lossen moet je dan inloggen en iets herstellen. Maar in plaats van dat je bij je bank inlogt, log je in op een goed nagemaakte kopie, waar je verder niets kunt. Maar hierdoor hebben de aanvallers wel je inloggegevens!



Figuur 14: Twee slachtoffers van phishing

**Opdracht 6.** Vorm een duo met een medeleerling. Open je mailbox en zoek samen of je een phishingmail kunt vinden. Meestal worden deze door je mailbox gedetecteerd en in de map 'Ongewenste mail', 'Spam' of 'Junk' gezet. Ervan uitgaande dat je iets vindt, beantwoord de volgende twee vragen. Waarom denk je dat dit een phishingmail is?

**Opdracht 7.** Bekijk onderstaande e-mail van de klantenservice van ING. Geef twee argumenten waar je aan kan zien dat hier sprake is van phishing.

Geachte ,

Uit onze administratie blijkt dat uw Mobiel Bankieren moet worden bijgewerkt.

**Waarom krijg je deze e-mail?**

Bij berichten die belangrijk zijn, krijg je een seintje van ons. We hebben geconstateerd dat uw Mobiel Bankieren niet voldoet aan de nieuwste veiligheidsstandaarden. Werk uw Mobiel Bankieren zo snel mogelijk bij om tijdelijke blokkade van uw Mobiel Bankieren te voorkomen.

**Mobiel Bankieren bijwerken**

Wij vragen uw in te loggen op Mijn ING en de stappen te volgen om uw Mobiel Bankieren bij te werken.

[Log in bij Mijn ING](#)

Met vriendelijke groet,

**Directeur Klantenservice**

*Opdracht 8. Google biedt een Phishing quiz aan via: <https://phishingquiz.withgoogle.com>. Doe deze test. In hoeveel gevallen had je het juiste antwoord gekozen?*

## 2.6 Malware

Malware is een samenvoeging van de woorden 'malicious' en 'software'. Dit betekent 'kwaadaardige software'. Het omvat alle programma's die ontwikkeld zijn met kwaadwillende bedoelingen. Malware is er in verschillende vormen en soorten. De meest voorkomende zijn:

- Trojan horse
- Virus
- Worm
- Spyware
- Adware
- Ransomware

Vaak wordt malware gebruikt voor aanvallen via een zogenoemde **zero day kwetsbaarheid**. Dit zijn kwetsbaarheden of zwakke plekken in software die nog niet bekend zijn bij de ontwikkelaar van de software. Omdat de zwakke plek nog niet bekend is bij de ontwikkelaar, is er geen mogelijkheid om direct een oplossing uit te brengen voor deze kwetsbaarheid.

### 2.6.1 Trojan Horse

Een Trojan horse (Nederlands: Trojaans paard), vaak afgekort tot trojan, is een malware-soort die vernoemd is naar het paard van Troje. Dit is een bekend verhaal uit de Griekse oudheid. Om de stad Troje te veroveren had het Griekse leger een gigantisch houten paard gemaakt. In dit paard waren soldaten verstopt. De inwoners van Troje dachten dat het paard een cadeau was

en haalden het naar binnen. Vervolgens waren de vijandige soldaten in de stad. Zij openden de poort van de stad, waarna het leger ongehinderd naar binnen kon.

Net zoals bij het 'echte' paard van Troje hebben gebruikers soms niet door dat ze malware binnenhalen. Dat komt doordat de malware verstopt zit in bijvoorbeeld een e-mailbijlage, een bijlage bij een chat of bij een download via een website. Als je die bewuste e-mailbijlage of het gedownloade bestand opent, activeer je automatisch de trojan.

Een Trojan horse is geen programma dat zichzelf verspreidt. Als je het eenmaal hebt, zal het schade aanbrengen aan je systeem of het systeem openzetten voor hackers. Maar de verspreiding vindt nagenoeg altijd plaats door mensen. Misschien stuur jij nietsvermoedend die bewuste mail ook wel door naar andere mensen!

### 2.6.2 Worm

In tegenstelling tot een trojan verspreidt een worm zichzelf wel automatisch. Daar komt de naam van dit type malware ook vandaan. Het idee van een worm is dat hij zich door alle computernetwerken en het internet heen 'wurmt' en zich op die manier verspreidt, bijvoorbeeld via e-mail of via bestanden.

Sommige wormen zijn niet gemaakt om schade aan te richten, zoals de Blaster worm in 2003. Deze worm bevatte onder andere het bericht: *"billy gates why do you make this possible ? Stop making money and fix your software!!"*.

Dit is een oproep aan Bill Gates, de toenmalige CEO van Microsoft, om de beveiliging van Windows te verbeteren. De aanwezigheid van deze worm zorgde ervoor dat een computer vaak een foutmelding gaf en na 60 seconden automatisch werd afgesloten.

Een andere bekende worm uit het verleden is de 'ILOVEYOU' worm. Deze worm is op 4 mei 2000 gestart en binnen 10 dagen waren er meer dan 50 miljoen systemen geïnfecteerd. Op dat moment was dit ongeveer 10% van alle systemen wereldwijd! Deze worm veranderde bestanden op het systeem en verspreidde zichzelf per e-mail. Hiervoor gebruikte de worm het adresboek van het mailprogramma Outlook. Automatisch verzond de worm een mail naar alle e-mailadressen in het adresboek, met zichzelf als bijlage.

Hoewel sommige wormen geen kwade bedoelingen hebben, vragen ze altijd netwerkcapaciteit om zichzelf te verspreiden. Zo heeft een worm dus altijd een negatieve invloed op een computernetwerk.

### 2.6.3 Virus

Een virus is geen zelfstandig programma, zoals een worm. In plaats daarvan besmet een virus bestaande software, net zoals een echt virus mensen kan besmetten. Het virus nestelt zich meestal in uitvoerbare bestanden of executables. Dat zijn de bestanden waarmee je software opstart. De besmette software richt vervolgens schade aan en verspreid zichzelf naar andere computers.

Ook een worm nestelt zich meestal in een bestand. Het verschil met een virus is dat een worm zelf een compleet computerprogramma is. Het bestand waarin het zit, is alleen de plek waarin de worm zich verbergt.

**Opdracht 9.** Welke van de volgende soorten malware verspreidt zichzelf? Kies uit:

A. Trojan horse



B. Worm

C. Virus

**Opdracht 10.** Welke van de volgende soorten malware is een computerprogramma?

A. Trojan horse

B. Worm

C. Virus

#### 2.6.4 Spyware en Adware

Spyware is een type malware dat informatie over het computergebruik probeert te achterhalen. Dit wordt vervolgens, vaak via internet, doorgegeven aan de maker van de spyware. Informatie waarnaar spyware op zoek is, kan zijn:

- Geïnstalleerde programma's;
- Bezochte websites;
- Welke e-mails worden verstuurd;
- Alle toetsenbordaanslagen.

Spyware zorgt ervoor dat het iedere keer wordt opgestart als een computer opnieuw wordt aanzet.

Adware is een andere categorie malware. De 'ad' van adware staat voor advertentie. Het doel van adware is dus het weergeven van advertenties op je computer.

Dit kan ook *legaal* zijn, bijvoorbeeld bij de installatie van shareware. Er kan dan regelmatig een advertentie komen waar je in wordt aangespoord om de volledige versie van het programma aan te schaffen.

Maar vaak wordt adware gebruikt om ongewenste reclames te geven. Vaak bevat adware ook technieken die in spyware zitten. Op die manier kan adware gerichte reclames aan de gebruiker voorschotelen.

Spyware en adware worden vaak gezien als eenzelfde soort malware. Maar ze hebben een andere functie, die in de praktijk wel vaak gecombineerd wordt.

#### 2.6.5 Ransomware

Ransomware is een speciaal soort malware, die vaak een systeem binnendringt als Trojan horse of door middel van een worm. Als ransomware eenmaal op een systeem staat, versleutelt het bestanden. Hierdoor zijn deze bestanden niet meer te gebruiken. Vervolgens verschijnt er een melding dat de gebruiker een geldbedrag moet betalen, om weer toegang te krijgen tot de versleutelde bestanden.

Er wordt over het algemeen aangeraden om geen geld over te maken. Ten eerste omdat het helemaal niet zeker is dat je inderdaad de toegang tot je bestanden terugkrijgt. Ten tweede omdat ransomware hierdoor een lucratieve methode is voor (internet)criminelen om aan geld te komen.

Ransomware is één van de nieuwste vormen van malware en wordt pas sinds 2012 actief ingezet. Toch is het in het verleden ook al voorgekomen, zoals bijvoorbeeld in het jaar 1989 in België. In de volgende video leer je hier alles over: <https://www.youtube.com/watch?v=ZXBLLIuVeXo>.

In april 2021 was een leverancier van Albert Heijn slachtoffer van een ransomware-aanval. De databaseservers van het bedrijf werden geïnfecteerd met ransomware. De leverancier was verantwoordelijk voor de levering van kaas aan de supermarkten. Omdat de bedrijfsvoering volledig stil kwamen te liggen, was er bij Albert Heijn tijdelijk vrijwel geen kaas meer te krijgen.



### Wegens een technische storing is er beperkte beschikbaarheid op de voorverpakte kaas

Wegens een technische storing is er beperkte beschikbaarheid op de voorverpakte kaas. De logistiek dienstverlener werkt er met man en macht aan het probleem zo snel mogelijk op te lossen en de beschikbaarheid snel weer op orde te krijgen. Onze excuses voor het ongemak.

Figuur 15: Een gevolg van ransomware

Een maand later wordt een belangrijke Amerikaanse oliepijpleiding stilgelegd. Het bedrijf achter de pijpleiding is getroffen door ransomware. Daardoor zijn de ICT-systemen die de leiding aansturen offline gehaald en werkt de leiding niet meer. Het gevolg is dat alle olie per vrachtwagen vervoerd moet worden, wat enorm veel geld kost.

Bij ransomware-aanvallen, zoals de hiervoor genoemde gerichte aanvallen, wordt vaak gebruik gemaakt van tijdsdruk. Het slachtoffer moet snel betalen, anders vernietigen de aanvallers de data definitief, of ze dreigen op een andere manier nog meer schade aan te richten. Daarom zijn slachtoffers vaak geneigd om - tegen het advies van de politie in - maar te betalen, zodat meer schade voorkomen kan worden.

Hierdoor komen criminelen eerder hun eigen beloftes na. Zo zorgen ze ervoor dat betalen de moeite waard is en blijft het een lucratieve bezigheid om ransomware te verspreiden. Gelukkig vinden onderzoekers steeds vaker foutjes in de ransomware, waardoor slachtoffers ook zonder betaling hun bestanden terug kunnen krijgen. Dat gebeurde bijvoorbeeld bij de ransomware WannaCry, waarover je meer ziet in de onderstaande video: <https://www.youtube.com/watch?v=etPizFNPupk>.

**Opdracht 11.** Welke van de volgende soorten malware is altijd een vorm van computercriminaliteit?

- A. Spyware
- B. Adware
- C. Ransomware

**Opdracht 12.** Welke van de volgende soorten malware installeren zich op een systeem?

- A. *Spyware*
- B. *Adware*
- C. *Ransomware*

**Opdracht 13.** Welke van de volgende soorten malware zorgt ervoor dat je niet meer met een systeem kunt werken?

- A. *Spyware*
- B. *Adware*
- C. *Ransomware*

**Opdracht 14.** Zoek online naar een voorbeeld van ransomware voor smartphones met Android. Beantwoord daarna de onderstaande vragen.

- (a) Hoe heet de ransomware?
- (b) Leg kort uit wat deze ransomware doet.
- (c) Wat kun je doen om van deze ransomware af te komen?

## 2.7 Woordenlijst

De volgende belangrijke termen kwamen voor in hoofdstuk 2.

- SQL-injectie - manipuleren van een database door een webformulier.
- man-in-the-middle aanval - af luisteren van een verbinding tussen twee apparaten (bijvoorbeeld via een openbaar WiFi-netwerk).
- HTTP - protocol voor datacommunicatie via internet, waarbij geen encryptie wordt gebruikt.
- HTTPS - protocol voor datacommunicatie via internet, waarbij wel encryptie wordt gebruikt (maar geen end-to-end encryptie).
- SSL-certificaat - een certificaat met geverifieerde informatie over de eigenaar van een website. Dit maakt HTTPS-communicatie mogelijk.
- end-to-end encryptie - een vorm van encryptie waarbij de data ook op de server versleuteld wordt opgeslagen, en dus alleen de zender en ontvanger het kunnen ontsleutelen.
- brute force - iets proberen te raden/ontdekken door alle mogelijkheden uit te proberen.
- social engineering - het gebruik van psychologische trucs om mensen iets te laten doen dat ze eigenlijk niet willen.
- phishing - slachtoffers proberen naar een valse website te leiden met het doel om informatie (zoals wachtwoorden) te stelen.
- malware - kwaadaardige software.
- zero day kwetsbaarheid - een zwakke plek in software die al bestaat sinds het product is ontwikkeld.

- trojan horse - malware in een zelfstandig programma die door de gebruiker zelf wordt binnengehaald en die schade aanbrengt zodra de gebruiker hem opent.
- worm - een zelfstandig (meestal kwaadaardig) programma dat zichzelf verspreidt via een computernetwerk.
- virus - malware zonder zelfstandig programma die andere bestanden infecteert en zichzelf verspreid via een computernetwerk.
- spyware - malware die informatie over computergebruik achterhaalt en doorgeeft aan de makers.
- adware - software (malware of legale software) met als doel om advertenties weer te geven op een computer.
- ransomware - software die bestanden versleutelt en ze pas weer ontsleutelt als het slachtoffer betaalt.

## 3 Aanvallers en verdedigers

### 3.1 Inleiding

In de digitale wereld zijn er veel soorten aanvallers en verdedigers. Die spelen een kat- en muis-spel: de verdedigers ontwikkelen steeds betere manieren van beveiliging, aanvallers verzinnen steeds nieuwe manieren om die te doorbreken.

Wie zijn de aanvallers en de verdedigers? De aanvallers noemen we al snel hackers. Maar dat is een verwarrende term. Want is een hacker hetzelfde als een internetcrimineel? Nee, er zijn ook hackers met goede bedoelingen. Die hackers zijn geen aanvallers, maar helpen juist om de verdediging te verbeteren. En er zijn ook overheden die hacken om terroristen op te sporen.

In dit hoofdstuk kijken we naar wat computercriminaliteit precies is. Daarna kijken we wat voor soorten aanvallers en verdedigers er zijn.

#### Leerdoelen:

- 1 Je kunt bij computercriminaliteit verschillende aanvallers en verdedigers benoemen.
- 2 Je weet wat ethische hackers zijn.
- 3 Je weet wat een 'zero day' is.

### 3.2 Computercriminaliteit

Er zijn heel veel vormen van **computercriminaliteit** of **cybercrime**. De belangrijkste daarvan zijn diefstal, fraude, afpersing en inbraak (hacken). Over de eerste drie soorten gaat deze paragraaf. Hacken is het onderwerp van de volgende paragraaf.

Er zijn veel beveiligingsbedrijven die gespecialiseerd zijn in het bestrijden van één van de vormen van computercriminaliteit. Met de juiste maatregelen kun je veel problemen voorkomen. In hoofdstuk 4 lees je welke maatregelen er genomen kunnen worden. Als je toch te maken krijgt met computercriminaliteit, is het verstandig om aangifte te doen bij de politie. Want criminaliteit heeft soms ernstige gevolgen.

In deze video zie je hoe de politie bezig is met cybercrime:  
<https://www.youtube.com/watch?v=DeNVV6XX0Fg>.

#### 3.2.1 Diefstal

**Diefstal** van data kan op veel manieren gebeuren. Bijvoorbeeld doordat een apparaat van jou wordt gehackt. Of omdat de dief toegang heeft tot een database waarin gegevens staan over jou. Als er diefstal is gepleegd, kan het gebeuren dat je daar helemaal niets van merkt.

Deze gestolen data is vaak geld waard en kan door de dief worden doorverkocht. Hij kan ook op andere manieren misbruik maken van je persoonlijke gegevens. Bijvoorbeeld door criminele activiteiten uit te voeren onder jouw naam. Dat heet **identiteitsfraude**. Als de crimineel dreigt om de persoonlijke gegevens openbaar te maken, tenzij je betaalt, noemen we dat afpersing.

#### 3.2.2 Fraude

**Fraude** is een vorm van oplichting: er wordt bedrog gepleegd, meestal met het doel om mensen geld afhandig te maken. Een bekend voorbeeld is phishing. Maar ook spyware kan het doel

hebben om bijvoorbeeld bankgegevens te achterhalen. Ook komt fraude voor via online shops, social media of online dating. Bijvoorbeeld als iemand geld betaalt voor een product, maar dat nooit ontvangt. Er zijn ook veel voorbeelden van slachtoffers die online een relatie opbouwen met iemand die helemaal niet blijkt te zijn wie hij zegt te zijn. Criminelen vragen dan aan het slachtoffer veel geld. Bijvoorbeeld door te zeggen dat ze het slachtoffer graag willen ontmoeten, maar geen geld hebben om de vliegreis te betalen.

### 3.2.3 Afpersing

Malware kan worden gebruikt voor **afpersing**. Ransomware is daarvan een bekend voorbeeld (paragraaf 2.5). Maar ook met gevoelige gegevens kan een crimineel een individu of bedrijf afpersen. Bijvoorbeeld door te dreigen die gegevens openbaar te maken als er niet wordt betaald. Ook dreigen om naaktfoto's van iemand te delen als dwangmiddel om die persoon iets te laten doen, is een vorm van afpersing. In dat geval kan er ook sprake zijn seksueel misbruik, wat nog veel verder gaat dan afpersing.

Vaak gebruiken criminelen hiervoor gestolen gegevens. Iemand haalt bijvoorbeeld jouw naam en e-mailadres uit een gestolen database en stuurt je een mail. Daarin beweert hij dat hij toegang heeft gekregen tot je webcam en bestanden. De beelden en bestanden dreigt hij naar je vrienden en familie te sturen, tenzij je een groot bedrag overmaakt. Gelukkig komt het bijna niet voor dat de persoon de beelden en bestanden daadwerkelijk heeft. Door je bang te maken, hoopt hij dat je betaalt.

***Opdracht 1.** Bedenk drie verschillende manieren waarop gevoelige data van jou gestolen zou kunnen worden. Bedenk eerst een aantal plekken waar er gevoelige data van jou staat opgeslagen. Bedenk daarna manieren waarop die gestolen kunnen worden. Als het eenvoudig is om je gevoelige data te stelen, doe er dan ook iets aan!*

## 3.3 Computervredereuk

Hacken is een van de grootste bedreigingen van cybersecurity. De wet noemt hacken **computervredereuk**. Er zijn aparte wetsartikelen voor computervredereuk, zowel in Nederland als in de Europese Unie. Die zijn speciaal gemaakt om allerlei vormen van criminaliteit te kunnen bestraffen. Computervredereuk is een misdrijf. Je kunt er in ernstige gevallen dan ook voor in de gevangenis belanden.

Maar wat is computervredereuk precies? Het is het ongeoorloofd binnendringen in een computersysteem of een netwerk. Met andere woorden: digitaal inbreken. Of de inbraak via een geavanceerde hackpoging gaat of omdat je simpelweg iemands wachtwoord hebt afgekeken, maakt niet uit. De wet zegt namelijk niets over de manier waarop dat kan gebeuren. Dat is ook logisch: er komen steeds nieuwe manieren van hacken bij. Die kunnen niet allemaal in de wet staan.

Niet alleen het binnendringen zelf is strafbaar. Ook het doen van een poging om binnen te dringen is verboden. Hacken is dus ook strafbaar als het mislukt. Zelfs als je zonder succes probeert in te loggen door iemands wachtwoord te gokken, ben je strafbaar.

Ook het bezitten van hulpmiddelen met het doel om te hacken, is strafbaar. Als je dus een keylogger of hacksoftware hebt, kan dat dus al strafbaar zijn. In de praktijk is het moeilijk vast te stellen of die hulpmiddelen bedoeld zijn om te hacken. De hacksoftware zou je ook kunnen gebruiken om je eigen systeem op veiligheid te testen.

En wat nu als een website of app slecht beveiligd is? Dat is geen vrijbrief om te hacken. Slechte beveiliging is overigens wel verwijtbaar. Als een slecht beveiligde website persoonsgegevens

bewaart, is de eigenaar van de website zelfs strafbaar. Maar een 'openstaande achterdeur', mag niet worden gebruikt om een systeem binnen te dringen. Zo'n beveiligingslek melden is wel toegestaan: dat is juist heel goed. Daarover lees je meer in de volgende paragraaf.

### 3.3.1 Na de inbraak

Als je hebt ingebroken in een computer, ben je dus schuldig aan computervrederebreuk. Dat is al zo, als je na de inbraak verder niets hebt gedaan. Als je daarna ook nog gegevens kopieert, verwijdert of wijzigt of op een andere manier schade aanbrengt, dan is dat een extra strafbaar feit.

**Opdracht 2.** Fox-IT is de bekendste Nederlandse securityspecialist. Je vindt hun site via <https://www.fox-it.com/nl>. Selecteer de diensten die Fox-IT aanbiedt. Kies uit:

- A. Forensisch onderzoek naar computercriminaliteit
- B. Het fysiek beveiligen van bijvoorbeeld serverparken
- C. Het ontwerpen van malware
- D. Het trainen van personeel op het gebied van security
- E. Het ontwerpen van veilige softwareprogramma's voor bedrijven
- F. Kwetsbaarheden in digitale infrastructuur opsporen

**Opdracht 3.** Ga op zoek naar bronnen die meer vertellen over computervrederebreuk. Welke straffen staan er op hacken?

## 3.4 Ethisch hacken

Na het lezen van de vorige paragraaf zou je kunnen denken dat hacken altijd een criminele bezigheid is. Maar gelukkig zijn er ook allerlei hackers actief die juist helpen om het internet veiliger te maken. We noemen hen **ethische hackers**.

Het is gevaarlijk als een beveiligingslek openbaar wordt. Criminelen zullen er direct proberen misbruik van te maken en zo kan er grote schade ontstaan. Ethische hackers melden een beveiligingslek daarom bij het betrokken bedrijf. Dat bedrijf wordt zo in staat gesteld om het lek te dichten. Veel bedrijven zijn blij met deze meldingen en geven de hacker er een beloning voor.

Hier zie je een video waarin een ethische hacker vertelt over hoe hij bij de overheid heeft ingebroken: <https://www.youtube.com/watch?v=sBOSqcBtGMM>.

Er zijn ook bedrijven die een beveiligingsprobleem niet of niet snel genoeg oplossen als het is gemeld. Ook dat is gevaarlijk, want gebruikers kunnen slachtoffer worden van het lek. Daarom is het soms verstandig om een lek wel openbaar te maken: de gebruikers worden zo gewaarschuwd.

De meeste hackers kiezen voor een tussenvorm: **responsible disclosure**. Eerst wordt het beveiligingslek gemeld bij degene die ervoor verantwoordelijk is. Na een bepaalde periode maakt de hacker het lek openbaar. Zo slaat de hacker twee vliegen in één klap. De verantwoordelijke wordt gedwongen het probleem snel op te lossen en de hacker krijgt alle eer voor het vinden van het lek.

In deze video zie je iets over een project in Rotterdam over ethisch hacken: <https://www.youtube.com/watch?v=ukrO48j-6uc>.

**Opdracht 4.** Bij veel bedrijven kun je online lezen hoe ze omgaan met ethische hackers. Bijvoorbeeld <https://www.thuisbezorgd.nl/bugbounty> en <https://www.rabobank.nl/particulieren/veiligbankieren/kwetsbaarheden-melden>. Gebruik de twee genoemde websites of zoek zelf een andere op. Gebruik de zoekterm 'responsible disclosure'.

- (a) Geef een voorbeeld van een soort kwetsbaarheid waarover het bedrijf graag een melding ontvangt.
- (b) Wat wil het bedrijf dat je doet als je een kwetsbaarheid gevonden hebt?
- (c) Wat mag je volgens het bedrijf niet doen?
- (d) Wordt er een beloning gegeven? Om wat voor soort beloning gaat het?
- (e) Zijn er aangewezen testomgevingen waarin je aan de slag kunt, zonder per ongeluk privégegevens in te zien?

### 3.4.1 Persvrijheid

Ook ethische hackers overtreden de wet door te hacken. Toch zullen ze niet worden vervolgd. Dat komt omdat ze een publiek belang dienen: het internet wordt er veiliger van. Maar dat is niet de enige reden waarom ze niet vervolgd worden. Het publiceren van informatie over gevaarlijke beveiligingsproblemen valt onder de persvrijheid. Het maakt daarbij niet uit of je journalist bent of niet.

Er gelden natuurlijk wel regels. Je mag alleen hacken als dat de enige manier is om een misstand aan te tonen. Die misstand moet ook ernstig genoeg zijn. En je moet het daarbij laten. Als je vervolgens ook nog onnodig gegevens steelt of onnodig veel computers hackt, word je daar wel voor vervolgd.

## 3.5 Spionage en oorlogsvoering

Een **zero day** is een nog niet ontdekte kwetsbaarheid. Zero days zijn belangrijke middelen die kunnen worden gebruikt om te hacken. Daarom zijn ze geld waard. Er bestaat veel handel in. Belangrijke zero days worden verkocht voor enkele tienduizenden tot wel honderdduizenden euro's.

Je kunt zero days beschouwen als de wapens van de digitale oorlogsvoering en de verkoop ervan als een vorm van wapenhandel. Want met zero days kunnen schadelijke aanvallen worden uitgevoerd, gegevens gestolen en systemen worden platgelegd.

Wie zijn er geïnteresseerd in zero days? Allereerst natuurlijk criminelen. Maar ook beveiligingsbedrijven kopen ze met het doel om de lekken te dichten. Het duurt namelijk vaak langer dan een jaar voordat een zero day aan het licht komt. Als beveiligingsbedrijven zero days kopen, weten ze ook welke systemen kwetsbaar zijn en kunnen ze hun klanten ertegen beschermen.

*Het is mogelijk om een zero day kwetsbaarheid aan te geven bij Zerodium (<https://www.zerodium.com/>). Deze organisatie handelt in zero days. Het biedt daar meestal hogere bedragen voor dan de makers van de software met de kwetsbaarheid. Vervolgens worden de kwetsbaarheden verkocht aan bedrijven en overheden. Die hebben daar helaas maar al te vaak slechte bedoelingen mee.*

*In april 2021 biedt Zerodium 2,5 miljoen dollar voor het vinden van een mogelijkheid om op afstand de controle over een Androidtoestel over te nemen, zonder tussenkomst van de gebruiker van die telefoon. Google zelf biedt 'slechts' enkele honderdduizenden dollars voor het melden van deze kwetsbaarheid.*



Ook overheden maken gebruik van zero days. Dat doen ze om te spioneren. Door vijandige systemen te hacken, kan waardevolle informatie worden verzameld. Ook kan een zero day worden gebruikt om belangrijke vijandelijke systemen plat te leggen.

Je kunt je afvragen of het niet beter is als overheden de kwetsbaarheden in een systeem melden bij de ontwikkelaar van dat systeem. Dan kan de kwetsbaarheid worden opgelost. Door zero days te gebruiken, blijft de kwetsbaarheid bestaan en wordt het internet onveiliger. Om deze reden is het gebruik van zero days omstreden. In Nederland mag de overheid zero days alleen onder strikte voorwaarden gebruiken.

*Het meest spectaculaire voorbeeld van het gebruik van zero days is de inzet van Stuxnet, malware die door de Amerikaanse en Israëlische inlichtingendiensten is ontwikkeld om het Iraanse kernprogramma te saboteren. Stuxnet bevatte verscheidene zero days, waardoor het mogelijk was om de software ongemerkt te installeren bij de Iraanse centrale bij Natanz. Daar zorgde de software er vervolgens voor dat de centrifuges, die werden gebruikt om uranium te verrijken, veel sneller of veel trager gingen draaien. Zo konden Amerika en Israël het Iraanse programma om kernwapens te ontwikkelen vertragen.*

Hier zie je een video waarin een ethische hacker vertelt over hoe hij bij de overheid heeft ingebroken: <https://www.youtube.com/watch?v=7g0pi4J8auQ>.

**Opdracht 5.** De groep Anonymous is in de afgelopen jaren berucht geworden door aanvallen op bedrijven, organisaties en overheden. Binnen deze groep zijn veel hacktivisten actief.

Welke definitie past het beste bij een hacktivist? Kies uit:

- A. Iemand die hackt om aandacht te vragen voor zijn of haar probleem
- B. Iemand die hackt om kwetsbaarheden in digitale beveiliging aan de kaak te stellen
- C. Iemand die hackt om kwaadaardige personen tegen te houden
- D. Iemand die hackt om actie te voeren voor of tegen principiële onderwerpen

**Opdracht 6.** Zoek naar het manifest van Anonymous. Wat is het doel van Anonymous?

- A. Het tegengaan van alle kwaad in de wereld
- B. Het tegengaan van alle vormen van censuur
- C. Het beter beveiligen van het gehele internet
- D. Tegenwicht aan de te machtige overheid bieden

**Opdracht 7.** Noem een voorbeeld van een aanval die Anonymous uitvoerde. Bereikte Anonymous met die aanval het doel dat het voor ogen had?

**Opdracht 8.** Wat vind je van de acties van Anonymous? Leg uit waarom.

### 3.6 Woordenlijst

De volgende belangrijke termen kwamen voor in hoofdstuk 3.

- computercriminaliteit/cybercrime - alle vormen van criminaliteit waar computers bij zijn betrokken.
- diefstal - het stelen van bijvoorbeeld data.
- identiteitsfraude - het uitvoeren van criminele activiteiten onder andermans naam.
- fraude - bedrog, met het doel om mensen geld afhandig te maken (bijvoorbeeld phishing).
- afpersing - ergens mee dreigen zodat iemand geld betaald (bijvoorbeeld met het openbaar maken van gevoelige informatie of met het vernietigen van bestanden).
- computervredebreuk/hacken - ongeoorloofd binnendringen in een computersysteem of een netwerk.
- ethisch hacken - hacken met het doel om een systeem veiliger te maken.
- responsible disclosure - een beveiligingslek eerst melden bij degene die er verantwoordelijk voor is, met de aankondiging dat het even later openbaar gemaakt zal worden.
- hacktivist - iemand die hackt met het doel om kwetsbaarheden in digitale beveiliging aan de kaak te stellen.
- Anonymous - een internationale organisatie van hacktivisten met als doel het tegengaan van alle censuur.

## 4 Maatregelen

Om de veiligheid van ICT-systemen goed te maken en te houden, zijn er veel partijen nodig die zich daarvoor inzetten: cybersecuritybedrijven, de overheid, softwareontwikkelaars en zeker ook de gebruikers. Er zijn heel veel verschillende maatregelen die zij kunnen nemen om de veiligheid van een systeem te vergroten. Deze maatregelen kun je verdelen in vier soorten: preventie, detectie, repressie en correctie. In de volgende paragrafen wordt uitgelegd wat die maatregelen inhouden.

Encryptie speelt een centrale rol in de beveiliging van gegevens. Hoe encryptie werkt, lees je in paragraaf 5 en 6. In de laatste paragraaf staan tips over wat je zelf kunt doen om je veiligheid te vergroten.

### Leerdoelen:

- 1 Je kunt de verschillende maatregelen tegen computercriminaliteit verdelen in preventie, detectie, repressie en correctie.
- 2 Van deze vier categorieën kun je voorbeelden noemen.
- 3 Je weet het verschil tussen symmetrische en asymmetrische encryptie.
- 4 Je weet wat je zelf kunt doen om de veiligheid van je computer te vergroten.

### 4.1 Preventie

**Preventieve** beveiligingsmaatregelen zijn de maatregelen die worden genomen om problemen te voorkomen. Dat begint bij hard- en software. Die moet veilig worden gemaakt en de software moet up-to-date blijven. Dat betekent bijvoorbeeld dat een softwareontwikkelaar op de hoogte moet zijn van manieren waarop je goed beveiligde software maakt.

Een voorbeeld van een softwaresecuritymaatregel is **sandboxing**. Deze techniek laat apps in hun eigen afgesloten ruimte draaien, waar ze alleen toegang krijgen tot hun eigen geheugen en opslag. De meeste apps hebben namelijk geen reden om toegang tot andere plekken in het systeem. Willen ze dat wel, dan moeten ze toestemming vragen aan het besturingssysteem. Op je telefoon zie je dit terug wanneer een app toegang vraagt tot bijvoorbeeld je camera, je bestanden of je locatie. In een sandbox kan malware geen schade aanrichten.

Goed ontworpen en onderhouden hard- en software hebben zo min mogelijk kwetsbaarheden. Op die manier maken indringers weinig kans. Toch moeten de juiste gebruikers wel eenvoudige toegang hebben. Goede authenticatie is dan natuurlijk essentieel. Maar ook is het belangrijk om alleen de echt noodzakelijke manieren van toegang toe te staan. Elke nieuwe mogelijkheid om een systeem in te komen, is immers een nieuwe plek waar zwakheden kunnen ontstaan.

*Uit onderzoek van De Volkskrant in 2018 bleek dat driekwart van alle websites van het midden- en kleinbedrijf kwetsbaar is voor inbraak. Het gaat dan om websites van bijvoorbeeld sportverenigingen, scholen, huisartsen, tandartsen, fysiotherapeuten en kinderdagverblijven. Die websites verwerken privacygevoelige gegevens van klanten, zoals rekeningnummers, burgerservicenummers of gegevens over de gezondheid van cliënten. In een kwart van de gevallen kunnen hackers redelijk eenvoudig toegang krijgen tot de databases met deze gegevens. De oorzaak van de problemen zijn onder andere open poorten, verouderde software en onbeveiligde verbindingen.*

Een andere belangrijke preventieve maatregel is de encryptie van gegevens als ze worden opgeslagen of verzonden. Als de versleutelde data in verkeerde handen terechtkomt, kan deze zeer

moeilijk worden ontsleuteld. Meer over encryptie lees je in paragraaf 5 en 6.

Het maken van back-ups is een belangrijke preventieve stap in de bescherming tegen verlies of onbedoelde wijziging van data. Ten slotte moeten gebruikers actief meewerken aan het voorkomen van problemen. Wat voor maatregelen dat zijn kun je lezen in de laatste paragraaf.

Wanneer een bedrijf persoonsgegevens verwerkt, is het wettelijk verplicht preventieve maatregelen te nemen om de gegevens te beschermen. Dat is vastgelegd in de Europese privacywetgeving. Verder moet het bedrijf uitleggen hoe het de gegevens beschermt. Op die manier kun jij als gebruiker zelf nagaan of je gegevens veilig worden bewaard, en goede keuzes maken waar je je gegevens wilt achter laten.

**Opdracht 1.** Kies een website waar jij persoonsgegevens achterlaat, zoals Facebook, Gmail of Instagram. Ga op zoek naar informatie over de maatregelen die de website neemt om je gegevens te beveiligen. Welke maatregelen worden er genomen?

**Opdracht 2.** In 2020 werd er een datalek bij de website Infectieradar aangetoond. Lees het nieuwsbericht hierover op <https://www.vpngids.nl/nieuws/datalek-infectieradar-toont-persoonsgegevens-gebruikers/>. Zijn de volgende stellingen juist of onjuist?

- (a) De makers van deze website hadden dit datalek kunnen voorkomen.
- (b) Dit datalek is het gevolg van verouderde software.

## 4.2 Detectie

Helaas is software niet perfect. Er zullen altijd kwetsbaarheden in zitten die kunnen worden misbruikt. Daarom is **detectie** nodig: controle op misbruik. Bijvoorbeeld door bij te houden hoe vaak er een inlogpoging wordt gedaan met een bepaalde gebruikersnaam. Als dat te vaak is, kan de gebruiker worden geblokkeerd. Om detectie mogelijk te maken, worden allerlei gegevens over het gebruik van het systeem gelogd.

Een belangrijk hulpmiddel is de **firewall**. Die scant al het binnenkomende netwerkverkeer. Alle datapakketten worden gecontroleerd op kwaadaardige gegevens. Ook kan een firewall controleren of het verkeer afkomstig is van een vertrouwde bron. Firewalls beschermen tegen hackers, malware en spam. Er zijn firewalls voor computers en voor netwerken.

Binnen netwerken is een **Intrusion Detection System** een belangrijke aanvulling op firewalls. Ook IDS onderzoekt al het dataverkeer in een netwerk. Bijvoorbeeld op hackpogingen of een DDoS-aanval. Een firewall controleert het dataverkeer 'aan de poort' en kan deze toelaten of tegenhouden. Een IDS onderzoekt het verkeer dat de firewall heeft doorgelaten en dat zich binnen het netwerk bevindt. Het controleert bijvoorbeeld of alles 'normaal' verloopt, op basis van statistieken. Zo kan ongewoon grote drukte wijzen op een aanval.

Een tweede belangrijk type detectiehulpmiddel is **anti-malwaresoftware**. Die scant een apparaat op malware en verwijdert die. Er bestaan grote databases die kenmerken bevatten van allerlei soorten malware. Deze gegevens helpt anti-malwaresoftware bij het vinden van de malware.

De Play Store en App Store controleren nieuwe software voordat het beschikbaar wordt. Bijvoorbeeld op malware of het verzamelen van ongeoorloofde gegevens van gebruikers.

**Opdracht 3.** Virustotal.com is een website waar je bestanden op virussen kunt controleren. Deze dienst is ooit overgenomen door Google. Als je een bestand hebt dat je niet vertrouwt, kun je het daar uploaden en laten controleren.

Ga naar <https://www.virustotal.com/> en upload een bestand, bijvoorbeeld iets wat je onlangs hebt gedownload. Is het bestand veilig? Zo niet, wat voor malware is er aangetroffen?

### 4.3 Repressie en correctie

Als er sprake is van een aanval of als er malware is aangetroffen, moeten er maatregelen worden genomen (**repressie**) en moet eventuele schade worden hersteld (**correctie**). Welke maatregelen nodig zijn, hangt sterk af van het soort aanval.

Als er malware wordt aangetroffen op een apparaat in een netwerk, kan het voldoende zijn als die wordt verwijderd door anti-malwaresoftware. Een DDoS-aanval die niet sterk genoeg is, kan tijdelijk zorgen voor een iets tragere website. En als een server niet meer beschikbaar is vanwege beschadigde data, een hackpoging of malware, kan er worden overgeschakeld op een back-upstelsel. Het beveiligingslek moet dan wel zo snel mogelijk worden gedicht.

Wanneer de problemen serieuzer zijn, zullen er systemen uitvallen of moeten worden uitgezet. Bijvoorbeeld om te voorkomen dat data in verkeerde handen valt. In dat geval is er vrijwel altijd ook financiële schade door de uitval van de systemen en door de correctiekosten.

**Opdracht 4.** In paragraaf 4.2 heb je je verdiept in een datalek van de website Infectieradar. Lees hier over de nasleep van het datalek. Zijn de volgende stellingen juist of onjuist?

- (a) De reactie van het ministerie is een vorm van correctie.
- (b) Gebleken is dat er meerdere datalekken in de website aanwezig waren, toen deze online was.

**Opdracht 5.** Welke oplossingen zijn geen voorbeeld van repressie of correctie? Kies uit:

- A. Criminelen betalen voor het verwijderen van ransomware
- B. Klanten informeren over het datalek
- C. De servers offline halen
- D. Aangifte bij de politie doen
- E. Nieuwe antivirussoftware installeren
- F. Medewerkers scholen over het voorkomen van cyberaanvallen

### 4.4 Symmetrische encryptie

Het versleutelen van gegevens is belangrijk om te voorkomen dat het in verkeerde handen komt. Encryptie is in alle tijden toegepast. En je hebt het vast zelf ook wel eens gedaan. Bijvoorbeeld door letters te veranderen. Stel dat je elke letter verandert door de letter die drie plaatsen verder in het alfabet staat. Dan wordt elke a een d, elke b een e, enzovoorts. Het woord encryptie wordt dan hqfubswlh. Je kunt er ook voor kiezen om niet drie, maar vijf letters verderop te kiezen: elke a wordt dan een f, b een j, enzovoorts.

Deze manier van encryptie heet **Cesar-encryptie** en is bedacht door Julius Caesar. Hij gebruikte dit om op een 'veilige' manier te communiceren met het leger. Voor meer informatie, zie: <https://nl.wikipedia.org/wiki/Caesarcijfer>.

Dat je elke letter vervangt door een volgende letter uit het alfabet, noemen we het algoritme. Dat is de manier waarop de encryptie werkt. Het aantal letters dat je 'vooruit schuift' in het alfabet, is de **sleutel**. Voor elke vorm van encryptie geldt dat je zonder de sleutel de oorspronkelijke zin niet terug kunt krijgen.

Bij encryptie is er continu sprake van een kat-en-muisspel tussen aanvallers en verdedigers. Aanvallers proberen encryptie te breken. Ze zoeken een manier om de oorspronkelijke zin te vinden, zonder dat ze de sleutel hebben. In het vorige voorbeeld zou een aanvaller bijvoorbeeld elke sleutel kunnen proberen tot er een leesbare zin terugkomt. Er zijn twee manieren om encryptie veiliger te maken. De sleutel kan slimmer gekozen worden, waardoor het zo veel tijd kost om de sleutel te vinden dat het de moeite niet waard is. Ook kan het algoritme verbeterd worden, zodat het heel moeilijk wordt om te kraken.

Het algoritme uit het voorbeeld is duidelijk aan verbetering toe, omdat het ongeacht de sleutel altijd eenvoudig is om de versleuteling te kraken. Moderne encryptiemethoden gebruiken algoritmes en sleutels die zeer moeilijk te kraken zijn.

Encryptie die gebruikmaakt van één sleutel, heet **symmetrische encryptie**. Die sleutel wordt zowel gebruikt voor het versleutelen als het weer ontsleutelen van de data. Een van de bekendste symmetrische encryptie-algoritmen is Advanced Encryption Standard (AES). Dit wordt bijvoorbeeld gebruikt om bestanden op een opslagmedium te versleutelen.

In deze video zie je uitgelegd hoe versleuteling je bestanden beschermt:  
<https://www.youtube.com/watch?v=hvww48FV4G0>.

**Opdracht 6.** *De Enigma machine was een belangrijk encryptieapparaat van de Duitsers dat werd gebruikt tijdens de Tweede Wereldoorlog. Zoek informatie op over deze machine. Waar werd de Enigma precies voor gebruikt? Kies uit:*

- A. Het berekenen van militaire strategieën.
- B. Het automatiseren van contact binnen het Duitse leger.
- C. Het versleutelen van berichten binnen het Duitse leger.
- D. Het ontsleutelen van berichten van vijandelijke legers.

**Opdracht 7.** *Welke methode werd bij de Enigma machine gebruikt om symmetrische encryptie mogelijk te maken? Kies uit:*

- A. Er waren codeboeken beschikbaar voor iedereen die berichten verstuurde en ontving.
- B. Er was één unieke sleutel die alle gebruikers kenden.
- C. De sleutel werd door de verzender telefonisch doorgegeven aan de ontvanger.
- D. De ontvangende Enigma machine kon de sleutel uit het bericht halen

**Opdracht 8.** *Welke oorzaken hebben ertoe geleid dat de geallieerden de Enigma konden kraken? Kies meerdere juiste antwoorden uit:*

- A. Duitse krijgsgevangenen hebben de werking prijsgegeven.
- B. Er zat een grote ontwerpfout in de machine.
- C. Bij toeval werd een code geraden.

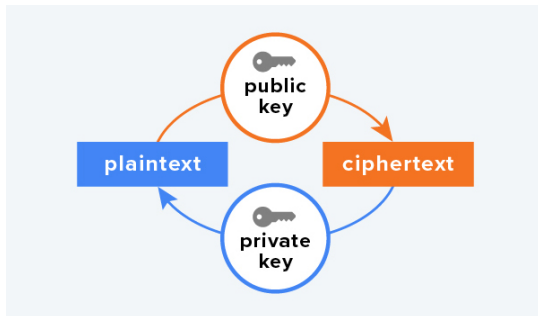
- D. De Duitse codes werden op een gegeven moment voorspelbaar.
- E. Er werd door duizenden mensen onderzoek gedaan naar de codes.
- F. De Enigma machine werd precies nagebouwd.

Als je dit onderwerp interessant vindt, kun je de film *The Imitation Game* uit 2014 bekijken.

## 4.5 Asymmetrische encryptie

Symmetrische encryptie is geschikt als de data niet hoeft te worden getransporteerd. De eigenaar hoeft de sleutel dan met niemand te delen en zo blijft die geheim. Bij het versturen van data over het internet is symmetrische encryptie ongeschikt. Want dan moet je de sleutel delen met de ontvanger. Anders kan de ontvanger niets met de versleutelde data. Het delen van een sleutel is riskant, want die kan worden onderschept.

Om dit probleem op te lossen, is asymmetrische encryptie bedacht. Dit wordt ook wel **public key encryptie** genoemd. Bij deze vorm van encryptie zijn er twee sleutels: een publieke en een geheime. Met de publieke sleutel wordt een bericht versleuteld. Met de geheime sleutel kan het versleutelde bericht weer worden ontsleuteld.



Figuur 16: Encryptie en decryptie met de private en public key

Iedereen mag de publieke sleutel weten. Dat is geen probleem, want je versleutelt er alleen maar mee. De geheime sleutel wordt nooit verspreid. Hoe werkt het precies? Alice wil een geheim bericht sturen naar Bob. Helaas luistert Eve alle communicatie af. Daarom moeten ze hun berichten versleutelen. Om dat te doen, kiest niet Alice (de verzender van het bericht), maar Bob (de ontvanger) een publieke sleutel én een geheime sleutel. Hij maakt de publieke sleutel openbaar, maar de geheime sleutel verspreidt hij niet.

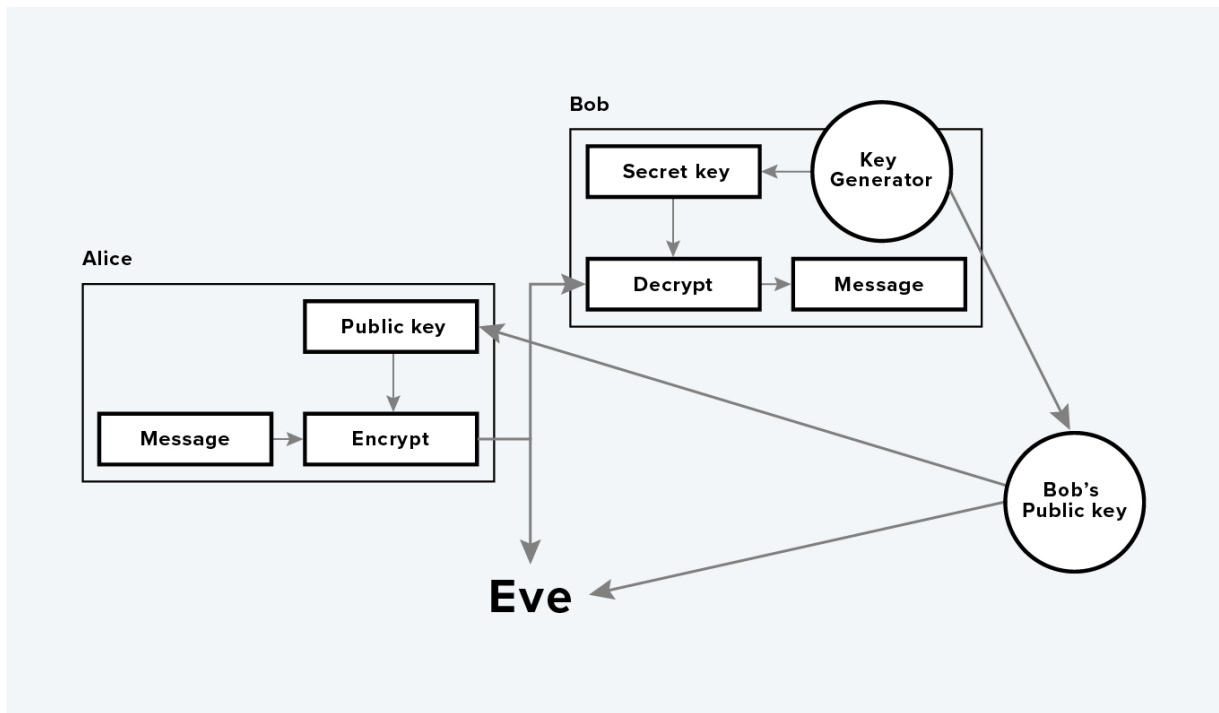
Eve en Alice kennen nu allebei de publieke sleutel. Alice versleutelt met die sleutel haar bericht en stuurt het naar Bob. Alleen Bob kan nu dat bericht ontsleutelen met zijn geheime sleutel. Omdat alleen Bob de geheime sleutel in bezit heeft, kan Eve de berichten niet ontsleutelen.

De publieke sleutel van Bob werkt als een soort hangslot waarvan alleen hij de sleutel heeft. Alice stopt het geheime bericht in een kistje. Daar maakt ze het hangslot aan vast. Dat kun je zonder sleutel doen. Nu kan uitsluitend Bob het kistje weer open maken, omdat alleen hij de sleutel heeft.

Public key encryptie wordt gebruikt bij vrijwel alle vormen van beveiligde data-overdracht. Denk maar aan een veilige internetverbinding via HTTPS.

**Opdracht 9.** Beantwoord onderstaande vragen over public key encryptie met ja of nee.

- (a) Kan Eve op dezelfde manier als Alice een bericht sturen naar Bob?



Figuur 17: Een schematische weergave van asymmetrische encryptie/decryptie

- (b) Kan Alice een veilig bericht naar Bob sturen zonder dat Bob daar vanaf weet?
- (c) Kan Bob met dezelfde publieke sleutel een veilig bericht terugsturen naar Alice?

Hoe asymmetrische encryptie werkt bij het versturen van berichten, en de mogelijke zwakke plekken die er zijn, zie je in de volgende video:  
<https://www.youtube.com/watch?v=TIldsUglGv4>

## 4.6 Wat kun je zelf doen?

De gebruiker is een heel belangrijke schakel in het beveiligingsproces. Als je bijvoorbeeld werkt met een verouderde webbrowser, dan heeft een hacker het wel heel gemakkelijk. Hoe goed de systemen die je gebruikt verder ook beveiligd zijn.

Wat kun je doen om de veiligheid te vergroten? Best veel en het hoeft ook niet ingewikkeld te zijn. Hieronder kun je lezen welke maatregelen je kunt nemen.

### 4.6.1 Absoluut noodzakelijk

We beginnen met de meeste basale maatregelen. Die zijn extra belangrijk. Als je ze (nog) niet genomen hebt, kun je dat het beste meteen doen.

- Installeer updates altijd direct. Als er een belangrijke kwetsbaarheid in software wordt ontdekt, dan zijn hackers daar ook van op de hoogte. Meestal zorgt de fabrikant binnen een dag voor een update die het lek dicht. Maar dan moet je die wel installeren, anders blijf je kwetsbaar.



- Zorg voor automatische vergrendeling van je smartphone, sim-kaart, tablet en computer. Anders kan een dief zonder moeite bij al je gegevens. Gezichtsherkenning (met infrarood) of een vingerafdrukscanner zijn het veiligst. Gebruik anders een wachtwoord of pincode.
- Gebruik sterke wachtwoorden (paragraaf 2.4) en vervang ze minimaal één keer per jaar. Gebruik niet overal hetzelfde wachtwoord. Het is lastig om veel wachtwoorden te onthouden. Je kunt daarom het beste een passwordmanager gebruiken (zie paragraaf 2.4).
- Zorg voor back-ups van je smartphone (een reservekopie) en van je belangrijkste gegevens. Je kunt er ook voor kiezen om je gegevens te bewaren in de cloud. Zorg ook voor de mogelijkheid om je smartphone op afstand te kunnen wissen. Als die dan gestolen wordt, kun je het de dief onmogelijk maken om ook nog je persoonlijke gegevens te stelen. Met de reservekopie kun je daarna alles terugzetten op een andere telefoon.
- Als je inlogt op een website, controleer dan of je een beveiligde verbinding hebt en of de website geen vreemde URL heeft. Gebruik nooit links in e-mails om in te loggen, maar vul zelf het adres in. Zo voorkom je dat je je gegevens invult op de verkeerde website.
- Download apps en andere software alleen vanuit de Play Store, App Store of van de website van een betrouwbare fabrikant. Als je het ergens anders vandaan haalt, kan het besmet zijn met malware. Twijfel je, laat het bestand dan scannen door een anti-malwareprogramma.
- Klik niet zomaar op gedeelde linkjes op social media, WhatsApp of e-mails. Het kan om phishing gaan of een link zijn naar een website met malware.

**Opdracht 10.** *Heb je zelf weleens te maken gehad met malware, een cyberaanval of een andere vorm van computercriminaliteit?*

- Beschrijf de situatie.*
- Wat heb je precies gedaan om deze situatie op te lossen?*
- Wat zou je anders hebben gedaan nu je dit hoofdstuk doorleest?*

#### 4.6.2 Verstandig om te doen

Er zijn nog meer maatregelen die je veiligheid vergroten. Die staan hieronder.

- Wees voorzichtig met openbare wifi-hotspots. Die kunnen gemakkelijk worden afgeluisterd. Log nooit ergens in zonder beveiligde verbinding. Voor extra veiligheid kun je gebruikmaken van een VPN-verbinding.
- Klik niet automatisch op 'ja' als een app om toegang vraagt tot bepaalde gegevens op je smartphone. Denk er even over na of dat echt nodig is en of je dat wel wilt.
- Installeer (extra) anti-malware- en anti-adwaresoftware op je smartphone en computer en stel in dat deze je apparaat regelmatig scannen. Als er dan malware of adware aanwezig is, wordt die automatisch verwijderd en krijg je een bericht.
- Als je data opslaat op een externe databron, zoals een externe harde schijf of USB-stick, versleutel dan de gegevens. In Windows bestaat daarvoor het programma BitLocker.
- Wees heel voorzichtig met het (permanent) aansluiten van zelfgeprogrammeerde apparaten op het internet, zoals een Arduino en Raspberry Pi. Deze apparaten zijn heel kwetsbaar voor automatische hacks. Via zulke hacks proberen criminelen software op je apparaat te installeren die bijvoorbeeld malware of spam verspreidt. Je moet behoorlijk veel technische kennis opdoen over de beveiliging van deze apparaten, voordat je ze veilig kunt verbinden met het internet.

**Opdracht 11.** Welke oplossingen pas jij zelf al toe? Kies uit:

- A. Verschillende wachtwoorden gebruiken
- B. Automatische vergrendeling van mijn smartphone
- C. Sterke wachtwoorden laten genereren door een webbrowser of programma
- D. Ik geef geen wachtwoorden af, ook niet aan bekenden
- E. Ik let op de URL's van datagevoelige websites
- F. Ik controleer of een Tikkie echt afkomt van de persoon die het 'verstuurt'

**Opdracht 12.** Lees dit artikel over het beveiligen van WhatsApp: <https://computertotaal.nl/artikelen/apps-software/beveiligingstips-voor-whatsapp/>. Welke oplossingen pas jij zelf al toe? Kies uit:

- A. Eén of meerdere privacyinstellingen
- B. Het maken van back-ups
- C. Tweestapsverificatie
- D. Beveiligingsmeldingen

## 4.7 Woordenlijst

De volgende belangrijke termen kwamen voor in hoofdstuk 4.

- preventie - maatregelen om problemen te voorkomen.
- sandboxing - een techniek die apps alleen in hun eigen afgesloten ruimte laat draaien, met alleen toegang tot eigen geheugen en opslag.
- detectie - controle op misbruik.
- firewall - software die al het binnenkomende netwerkverkeer scant op kwaadaardige gegevens.
- intrusion detection system - software die al het dataverkeer binnen een netwerk onderzoekt op kwaadaardige gegevens.
- anti-malwaresoftware - software die een apparaat scant op malware en die verwijdert.
- repressie - maatregelen die genomen worden zodra er een aanval of malware is gevonden.
- correctie - herstellen van schade na een (cyber)aanval.
- symmetrische encryptie - encryptie die gebruikt maakt van één sleutel voor zowel versleutelen als ontsleutelen.
- Ceaser-encryptie - encryptie waarbij elke letter een vast aantal letters 'verder wordt gedraaid' in het alfabet.
- asymmetrische encryptie (ook wel: public key encryptie) - encryptie waarbij data wordt versleuteld met een public key maar wordt ontsleuteld met een private key.

## 5 Verdieping: SQL-injecties

Scholengemeenschap Were Di en haar personeel zijn onder geen enkele voorwaarde verantwoordelijk voor de informatie en de kennis die door middel van deze verdiepingsmodule kan worden opgedaan.

### 5.1 Inleiding

Af en toe komt er een website of dienst in het nieuws die is gehackt door middel van SQL-injecties. Zie bijvoorbeeld <https://nos.nl/zoeken/?q=sql> of <https://tweakers.net/zoeken/?keyword=sql+injectie>. In deze verdiepingsmodule wordt uitgelegd:

- wat een SQL-injectie is;
- hoe een SQL-injectie kan worden uitgevoerd;
- hoe een programmeur kan zorgen dat zijn applicaties niet vatbaar zijn voor SQL-injecties.

Bekijk de volgende video: <https://www.youtube.com/watch?v=wcaiKgQU6VE>.

Verreweg de meeste websites zijn niet (meer) vatbaar voor SQL-injecties, maar sommige oudere websites nog wel. De PHP-scripts die in deze verdiepingsmodule worden gebruikt, zijn speciaal ontwikkeld om de werking van een SQL-injectie te kunnen bespreken.

SQL-injecties kunnen verstrekken gevolgen hebben voor een website, bijvoorbeeld als er gegevens in de database worden gewijzigd of worden verwijderd. De volgende cartoon onderstreept dit op ludieke wijze.

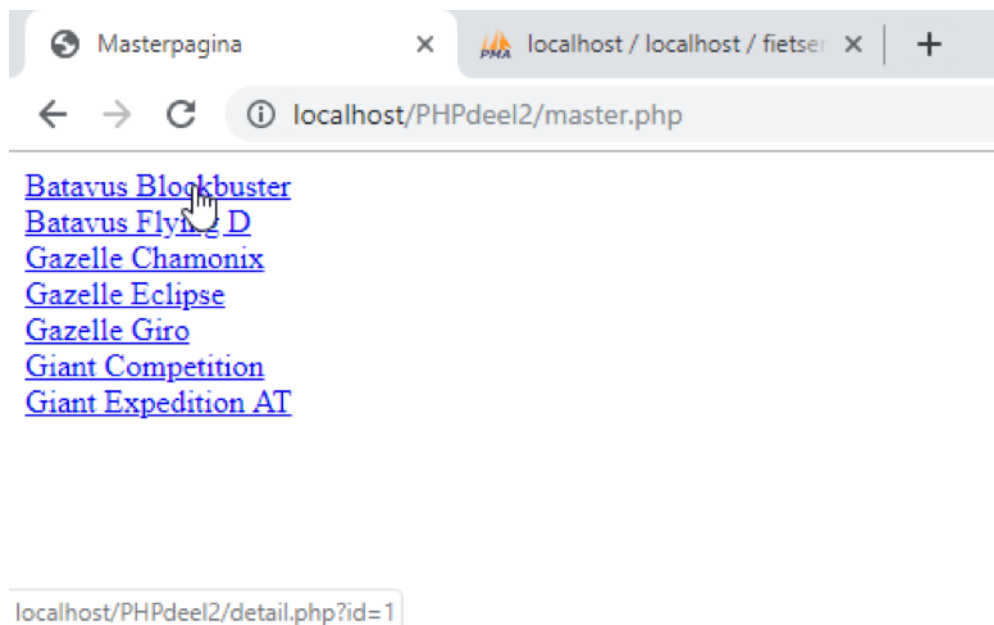


Figuur 18: Afkomstig van: <https://xkcd.com/327/>

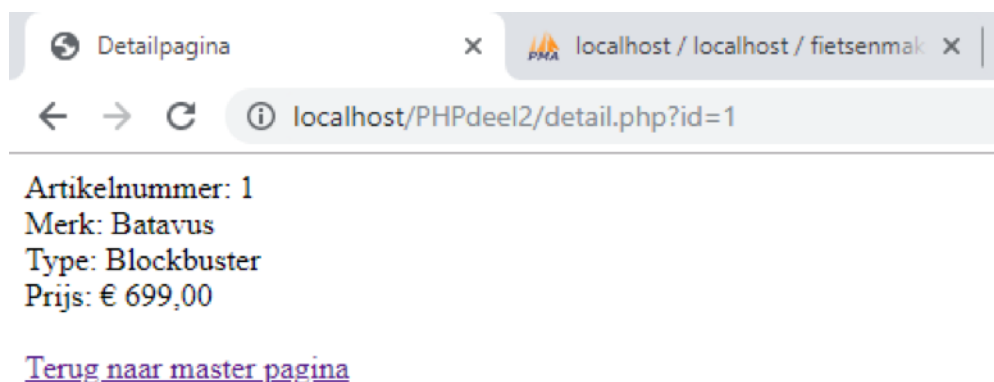
## 5.2 Wat is een SQL-injectie?

In het onderdeel 'Databases en SQL' heb je meer geleerd over de vraagtaal SQL. In PHP kun je SQL-code gebruiken om op een webpagina (een deel van) de inhoud van een databasetabel weer te geven.

Een webpagina kan aan de hand van gegevens in de URL specifieke gegevens uit de database opvragen. Bekijk het volgende voorbeeld. Op de 'Master pagina' staat een overzicht van een aantal fietsmerken. Als je op één van deze fietsmerken klikt, wordt de pagina 'detail.php' geopend. In de URL van deze pagina staat het artikelnummer van de fiets, zodat de detailpagina de gegevens van de juiste fiets kan tonen.



Figuur 19: De master-pagina



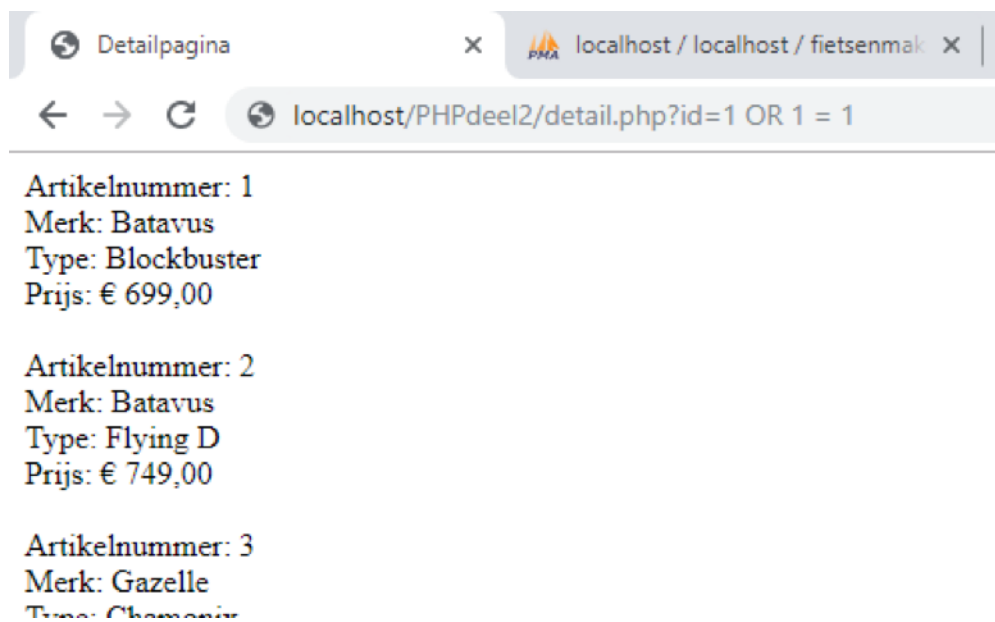
Figuur 20: De detail-pagina

Hackers of andere kwaadwilligen kunnen achter dit artikelnummer nog andere codes plaatsen. Hierdoor kan de inhoud van de detailpagina er opeens heel anders uit gaan zien. Dit wordt een SQL-injectie genoemd. Er wordt extra SQL in de pagina 'geïnjecteerd'.

Bekijk het volgende voorbeeld. Stel dat een kwaadwillende persoon van de URL `detail.php?id=1` de volgende URL maakt:

`detail.php?id=5 OR 1 = 1`

Nu wordt deze toevoeging ook meegenomen in de query op de detailpagina. De uitvoer van de detailpagina is nu hierdoor opeens heel anders...



### 5.3 Een SQL-query manipuleren

We gaan verder aan de hand van het voorbeeld in de vorige paragraaf. Door het toevoegen van `OR 1 = 1` in de URL worden nu opeens alle fietsen weergegeven. Maar wat gebeurt er precies?

De SQL-query die normaal gesproken wordt uitgevoerd, zou als volgt kunnen zijn:

```
SELECT *  
FROM fietsen  
WHERE id = nummer_uit_URL
```

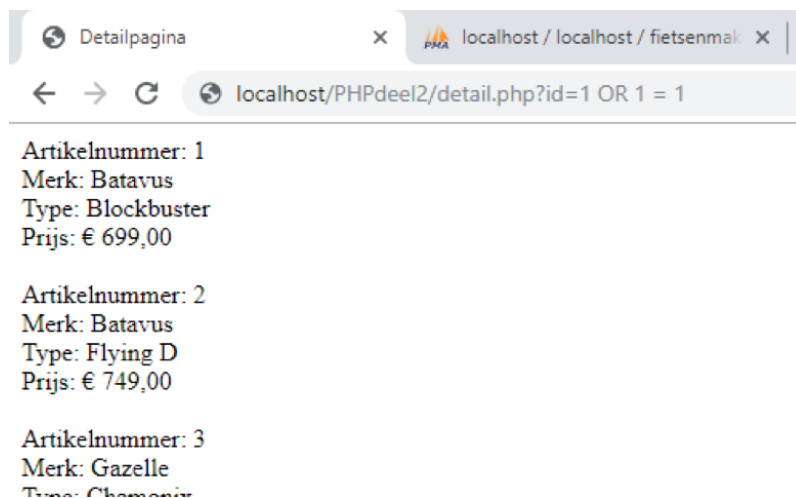
Op de plaats van `nummer_uit_URL` komt het artikelnummer uit de URL te staan. Hierdoor worden de artikelgegevens van de fiets met dit specifieke artikelnummer weergegeven. Met de toevoeging `OR 1 = 1` wordt de query als volgt:

```
SELECT *  
FROM fietsen  
WHERE id = nummer_uit_URL OR 1 = 1
```

Voor iedere rij in de database wordt de voorwaarde die genoemd is bij `WHERE` gecontroleerd. Er vinden nu twee controles plaats, namelijk:

- Is het id in de database gelijk aan het artikelnummer uit de URL?
- Is het getal 1 gelijk aan het getal 1?

Met het keyword `OR` moet één van de twee voorwaarden (of beide) waar zijn, wil een rij worden opgenomen in het resultaat. Aangezien de tweede voorwaarde altijd waar is - immers, 1 is logisch gezien altijd gelijk aan 1 - worden alle rijen weergegeven in het resultaat.



Figuur 21: De detail-pagina




Het bovenstaande voorbeeld is vrij onschuldig. In plaats van één fiets, worden er tientallen fietsen weergegeven. Alleen is het principe van een SQL-injectie (soms) ook toe te passen op een inlogpagina. Als het een hacker lukt om in te loggen, kunnen de gevolgen niet te overzien zijn.

Bekijk het volgende inlogformulier en de achterliggende databasetabel.

Gebruikersnaam:

  
  
Wachtwoord:  
  

Figuur 22: Inlogformulier

		id	user	pass	email
<input type="checkbox"/>		1	bob	geheim	bob@example.com
<input type="checkbox"/>		2	John	12345	john@example.com
<input type="checkbox"/>		3	Ann	ann123	ann@example.com

Figuur 23: Databasetabel

Bij de controle van de gegevens in het inlogformulier kun je de volgende query gebruiken:

```
SELECT *  
FROM members  
WHERE user = "gebruikersnaam_veld"  
AND pass = "wachtwoord_veld"
```

Als deze query een resultaat oplevert, zijn de ingevoerde gegevens juist.

Om het inlogformulier te 'kraken' is het mogelijk om gebruik te maken van de eerder besproken methode OR 1 = 1. Alleen moet er in dit geval wel een en ander worden toegevoegd aan de SQL-injectie. Dit in tegenstelling tot het voorbeeld van het fietsenoverzicht. De ingevoerde gebruikersnaam en het wachtwoord worden gezien als een string, een stuk tekst. Daarom worden deze waarden in SQL tussen aanhalingstekens geplaatst (in tegenstelling tot het artikelnummer uit het vorige voorbeeld; dat een getal is).

Bekijk het volgende voorbeeld:

Gebruikersnaam:

  
  
Wachtwoord:

Als deze gegevens worden verzonden, wordt de query als volgt:

```
SELECT *  
FROM members  
WHERE user = "a OR 1 = 1"  
AND pass = "a OR 1 = 1"
```

Aangezien de SQL-injectie nu tussen de aanhalingstekens staat, zal dit geen resultaat opleveren. Een oplossing hiervoor is om in de SQL-injectie ook aanhalingstekens te gebruiken, bijvoorbeeld:

Gebruikersnaam:

Wachtwoord:

Verzenden

De query wordt nu als volgt:

```
SELECT *  
FROM members  
WHERE user = "a" OR 1 = 1"  
AND pass = "a" OR 1 = 1"
```

Dit zal echter nog steeds geen resultaat geven. Er staat nu een aanhalingsteken achter de eerste OR 1 = 1. Om dit op te lossen kun je een hekje (#) toevoegen. Een hekje is het teken voor commentaar in SQL, waardoor alles wat na het hekje staat niet meer wordt meegenomen bij de uitvoer van de query. Als je een hekje in het gebruikersnaamveld invoert, maakt het niet meer uit wat er in het wachtwoordveld staat. Omdat die inhoud na het hekje aan de query wordt toegevoegd, wordt het niet meer uitgevoerd. Zie het volgende voorbeeld:

Gebruikersnaam:

Wachtwoord:

Verzenden

De query wordt nu:

```
SELECT *  
FROM members  
WHERE user = "a" OR 1 = 1#"  
AND pass = "a" OR 1 = 1"
```



Door het toevoegen van het hekje, is de query die door de database wordt uitgevoerd:

```
SELECT *  
FROM members  
WHERE user = "a" OR 1 = 1
```

Deze query heeft een resultaat, namelijk alle rijen van de tabel, waardoor we succesvol worden ingelogd!

## 5.4 De structuur van een database achterhalen

Naast het manipuleren van productoverzichtpagina's of het omzeilen van een inlogformulier, is het met een SQL-injectie soms ook mogelijk om meer inzicht te krijgen in de structuur van een database. Zo is het onder andere mogelijk om de naam van de database te achterhalen. En om namen en velden in een databasetabel te ontdekken. Deze manier werkt alleen als foutmeldingen van de database direct worden weergegeven, wat gelukkig steeds minder het geval is.

Als je een inlogformulier op een website ziet, is nog niet duidelijk welke databasestructuur hierachter zit. Al ligt het wel voor de hand dat in de databasetabel ten minste velden voor de gebruikersnaam, het wachtwoord en waarschijnlijk ook een e-mailadres voorkomen.

Door een SQL-injectie op het inlogformulier wordt de volgende query gegenereerd:

```
SELECT *  
FROM members  
WHERE user = "a" OR username = 1
```

Mogelijk komt nu de volgende SQL-error op de webpagina te staan:

*Unknown column 'username' in 'where clause'*

Uit deze foutmelding blijkt dat er geen kolom is in de databasetabel met de naam 'username'. Als met een SQL-injectie op het inlogformulier de volgende query wordt gegenereerd:

```
SELECT *  
FROM members  
WHERE user = "a" OR members = 1
```

Dan kan het zijn dat er geen SQL-error meer verschijnt. Hieruit kun je de conclusie trekken dat de kolom 'members' bestaat in deze databasetabel.

Via deze manier is het mogelijk om alle kolommen in de databasetabel te ontdekken. Het is alleen nog niet bekend wat de naam van de databasetabel zelf is. Gebruikersgegevens worden over het algemeen opgeslagen in een tabel met een naam als 'gebruikers', 'users', 'members' enzovoort. De SQL-injectie voor het achterhalen van de tabelnaam werkt op de zelfde manier als het achterhalen van de kolommen. Bekijk het volgende voorbeeld:

```
SELECT *  
FROM members  
WHERE user = "a" OR gebruikers.user = 1
```

Door vóór de kolomnaam in de SQL-injectie een mogelijke tabelnaam op te geven, is het mogelijk om te testen wat de naam van de databasetabel is. Aangezien we al weten dat de kolom 'user' bestaat, is een mogelijke foutmelding daarop niet van toepassing. Als deze query een error geeft

als:

*Unknown column 'gebruikers.user' in 'where clause'*

Dan is het duidelijk dat de naam van de databasetabel in ieder geval niet 'gebruikers' is. Als er na enige tijd proberen geen SQL-error meer wordt weergegeven, dan heb je waarschijnlijk de juiste naam voor de databasetabel gekozen.

Het achterhalen van de naam van de databasetabel en andere mogelijke databasetabellen in de database kun je ook in één keer doen met de volgende SQL-injectie:

```
SELECT *  
FROM members  
WHERE user = "a" AND 1 = (SELECT COUNT(*) FROM producten);
```

In dit voorbeeld wordt gebruik gemaakt van een subquery waarin het aantal rijen uit een andere databasetabel wordt geselecteerd. Nu gaat het er niet om te weten hoeveel rijen er in de andere tabel staan (wat overigens niet wordt weergegeven, mocht de SQL-injectie goed zijn). Het gaat ons om het feit of een SQL-error verschijnt of niet.

Mogelijk verschijnt de volgende SQL-error bij deze SQL-injectie:

*Table 'injections.producten' doesn't exist*

Hieruit blijken gelijk twee dingen. De database waarin de databasetabellen zitten, heeft als naam 'injections' én de databasetabel 'producten' bestaat niet. Als er geen SQL-error verschijnt, blijkt dat de gekozen naam voor de databasetabel bestaat in deze database.

Met deze methode kun je ook ontdekken welke kolommen er in een andere databasetabel staan. In plaats van COUNT(\*), dat altijd werkt, moet een kolomnaam worden opgegeven. Als er een SQL-error verschijnt, bestaat de kolom niet. Verschijnt er geen SQL-error, dan bestaat de kolom wel.

Deze truc hoeft niet alleen te werken bij een inlogformulier, maar kan ook werken bij het voorbeeld van het fietsenoverzicht. In dit voorbeeld heb je een SQL-injectie in de URL geplaatst.

## 5.5 SQL-query's uitbreiden

De SQL-injecties die tot nu toe zijn besproken waren allemaal relatief gezien onschuldig. Dat wil zeggen, er is geen schade ontstaan aan de database. Maar het is ook mogelijk om de gegevens in de database aan te passen: om er nieuwe gegevens aan toe te voegen, of om gegevens te verwijderen.

Stel dat de SQL-injectie om in te loggen niet werkt. Je kunt dan ook proberen om de gegevens in de database aan te passen naar gegevens die voor jou wel bekend zijn. Hierbij is het handig om een gebruikersnaam te hebben die zich al in de database bevindt. Het kan lastig zijn om daar achter te komen. Maar soms is een gebruikersnaam een e-mailadres. En je kent mensen waarvan je weet dat ze kunnen inloggen en welk e-mailadres ze hebben. Stel je voor dat je zeker weet dat de gebruikersnaam 'Bob' in de database voorkomt. Dan kun je de volgende SQL-injectie gebruiken om het wachtwoord van Bob aan te passen (ervan uitgaande dat je de naam van de databasetabel en enkele kolomnamen weet):

```
a"; UPDATE members SET pass = 'geheim' WHERE user = 'Bob'; #
```

De query die wordt uitgevoerd voor de controle van de gebruikersnaam en het wachtwoord, wordt nu:

```
SELECT *  
FROM members  
WHERE user = "a"; UPDATE members SET pass = 'geheim' WHERE user = 'Bob';#"
```

Wat gebeurt er allemaal? De query bestaat nu uit twee aparte query's, gescheiden door een punt-komma. Eerst wordt er gekeken of de gebruikersnaam gelijk is aan 'a', hoewel dat ongetwijfeld niet waar is. Daarna worden er in de database-tabel 'members' gegevens aangepast, en wel het wachtwoord van gebruiker Bob. Nu is het mogelijk om zonder SQL-injectie in te loggen, omdat we nu het wachtwoord van Bob weten.





Een andere SQL-injectie is om zelf een nieuwe gebruiker toe te voegen. Dit kan met de volgende SQL-injectie:

```
a "; INSERT INTO members (user, pass, email)  
VALUES('Peter', 'peter1995', 'peter@example.com');#
```

De query die wordt uitgevoerd voor de controle van de gebruikersnaam en het wachtwoord, wordt nu:

```
SELECT *  
FROM members  
WHERE user = "a"; INSERT INTO members (user, pass, email)  
VALUES('Peter', 'peter1995', 'peter@example.com');
```

In de databasetabel 'members' is nu een nieuwe gebruiker geplaatst. Als de databasebeheerder zou kijken welke gegevens er in de tabel 'members' staan, zou hij het volgende zien:

		id	user	pass	email
<input type="checkbox"/>		1	bob	geheim	bob@example.com
<input type="checkbox"/>		2	John	12345	john@example.com
<input type="checkbox"/>		3	Ann	ann123	ann@example.com
<input type="checkbox"/>		4	Peter	peter1995	peter@example.com

## 5.6 Wat is er tegen te doen?

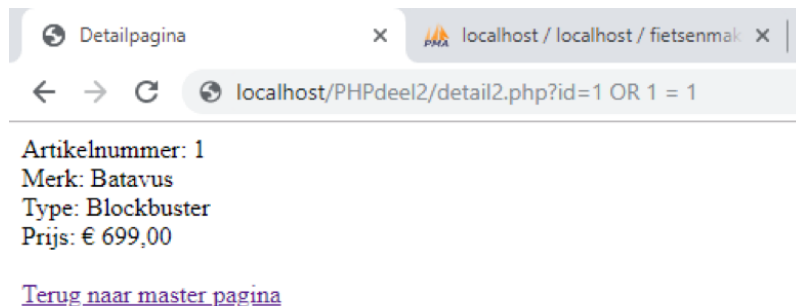
In de voorbeelden uit de vorige paragrafen zijn gegevens uit de URL of een formulier direct in de query geplaatst. Dit is een handige methode, maar óók een zeer onveilige methode. Dat bleek wel uit de extra codes die je met de SQL-injecties kon uitvoeren.

Om dit probleem op te lossen, moeten de gegevens uit de URL of uit een formulier op een speciale manier aan je query worden toegevoegd. Bekijk de volgende PHP-code:

```
1 <?php
2 $db = new PDO("mysql:host=localhost;dbname=fietsenmaker", "root", "root");
3 $query = $db->prepare("SELECT * FROM fietsen WHERE id = :id");
4 $artikelnummer = filter_input(INPUT_GET, "id", FILTER_SANITIZE_NUMBER_INT);
5 $query->bindParam("id", $artikelnummer);
6 $query->execute();
7 $result = $query->fetchAll(PDO::FETCH_ASSOC);
```

In de query worden de gegevens uit de URL vervangen door een zogenoemde 'placeholder'. Door middel van de functie `bindParam` is het mogelijk om deze placeholders te voorzien van de juiste data. De naam van een placeholder in een query mag je zelf kiezen. Voor de naam geef je een dubbele punt (:) op, zodat de database weet dat dit een placeholder is. De eerste parameter van de functie `bindParam` is de naam van de placeholder (zonder dubbele punt!) en de tweede parameter is de waarde waardoor de placeholder vervangen moet worden.

Als dezelfde SQL-injectie nu weer wordt uitgevoerd, wordt alleen het item met `id = 1` weergegeven:



Het gebruik van placeholders is een relatief veilige methode om invoer van gebruikers aan een query toe te voegen. Nog beter is het om dit te combineren met **opschoonfilters**.

De PHP-functie `filter_input` kun je gebruiken om waarden die je via de URL of een formulier ontvangt te filteren. Als parameters geef je op welke waarde je wilt controleren en waaraan deze waarde moet voldoen.

Op de vierde regel wordt de functie `filter_input` gebruikt. Deze functie heeft drie parameters. De eerste is de bron van de input. Als de gegevens uit de URL komen is dit `INPUT_GET`. Komen de gegevens uit een formulier, dan is dit `INPUT_POST`. Vervolgens geef je de naam op van het element waarvan je de ingevoerde waarde wilt opschoonen. In dit voorbeeld is dat 'id'. Als laatste geef je het type filter op. In dit voorbeeld zal er van de invoer een geheel getal gemaakt worden. Dat betekent dat als er letters of speciale tekens worden ingevoerd, deze worden verwijderd.

Er zijn nog meer filters die je kunt gebruiken, bijvoorbeeld voor:

- Een kommagetal
- Een stuk tekst
- Een e-mailadres
- Een webadres

Je leest er meer over op de website van PHP:

<https://www.php.net/manual/en/filter.filters.sanitize.php>.

Een ander belangrijk punt is om bij een PHP-script alleen tijdens het testen gebruik te maken van gedetailleerde foutmeldingen, waarin kolom- of databasenames te zien zijn. Een potentiële hacker kan aan de hand van een SQL-error de databasestructuur achterhalen. Het is beter om, als er een SQL-error optreedt, een eigen gemaakte foutboodschap te geven, bijvoorbeeld 'Er is een probleem met de database'.

## 6 Antwoorden

### 6.1 Digitale veiligheid

**Opdracht 1.** Andere voorbeelden kunnen onder andere zijn:

- het antwoord op een geheime vraag (iets wat je weet)
- een mobiele telefoon waarop een identificatiecode komt (iets wat je hebt)
- je stem, voor toegang met je een bepaald woord of zin zeggen (iets wat je bent)

**Opdracht 2.** Voor de identificatie worden kenmerken van je ID-kaart of paspoort geïdentificeerd. Bijvoorbeeld je naam en je BSN. Dit wordt vergeleken met de gegevens die in het systeem van de luchtvaart-maatschappij staan: de verificatie. Op die manier wordt gecontroleerd of de persoon die het ticket besteld heeft, ook echt voor de incheckbalie staat. Is het niet gelukt? Denk er nog eens over na.

**Opdracht 3.** Om op Twitter een verified account te krijgen, moet je een verzoek indienen bij <https://verification.twitter.com/welcome>. Een uitgebreide uitleg staat hier: <https://nl.wikihow.com/Een-geverifieerd-account-krijgen-op-Twitter>.

**Opdracht 4.**

- (a) Je kunt als leerling de gebruikersnaam makkelijk achterhalen. Stel dat je daarna het wachtwoord zou afkijken, dan zou je cijfers kunnen aanpassen.
- (b) Waarschijnlijk moet je docent een code invoeren die op zijn telefoon staat, of hij maakt gebruik van een afzonderlijk apparaat waarop een code verschijnt. Dat is een vorm van two factor authentication: je moet iets weten (zijn wachtwoord) en hebben (zijn telefoon of het apparaat). Het is dus een veilige manier van authenticatie. Weet je de telefoon of het code-apparaat van de ander te bemachtigen, dan is deze manier natuurlijk niet meer veilig.

**Opdracht 5.** De boarding pass is de eerste authenticatie (iets wat je hebt). Je paspoort is een tweede authenticatiemiddel (ook iets wat je hebt). Op het paspoort staan allerlei kenmerken van jou. Die kunnen worden gecontroleerd. Bijvoorbeeld op hoe je eruit ziet (iets wat je bent).

**Opdracht 6.**

- (a) Ja.
- (b) Ja.
- (c) Nee.
- (d) Ja.

Voor two factor authentication heb je twee verschillende vormen van authenticatie nodig. Je hebt dus iets nodig wat je weet of wat je bent. Een sleutel is iets wat je hebt. De schoolpas is ook iets wat je hebt, dus dat is geen goede two factor authentication. Een vingerafdruk is een voorbeeld van iets wat je bent. Een pincode is iets wat je weet. De beveiliging controleert jou op iets wat je weet (bijvoorbeeld je leerlingnummer) of op je pasfoto (iets wat je bent).

**Opdracht 7.** In de praktijk zal dit niet gebeuren omdat het te duur is. Een echte two factor authentication zorgt er ook voor dat je minder makkelijk een klasgenoot die je vertrouwt spullen uit je kluisje kunt laten halen.

**Opdracht 8.**

- (a) Bij een ELO heb je beheerders, docenten en leerlingen. In sommige gevallen is er ook de rol van ouder of verzorger, of van conciërge of baliemedewerker.
- (b) Beheerder: lesgroepen importeren, leerlingen verwijderen die van school zijn. Docenten: taken aanmaken voor leerlingen, berichten versturen, cijfers invoeren. Leerlingen: taken inleveren, cijfers inzien, rooster bekijken. Ouder/verzorger: heeft alleen leesrechten, kan niets inleveren en heeft beperkt toegang, bijvoorbeeld tot de cijfers of het rooster van de eigen kinderen. Conciërge of baliemedewerker: te laat-briefjes maken, roosters bekijken.

**Opdracht 9.** Installeer eerst een programma waarmee je de checksum kunt bepalen. Kies bijvoorbeeld een afbeelding of een Word-document. Als je een .exe-bestand kiest, kan je die niet via de mail delen met een klasgenoot.

Om de checksums te vergelijken is het handig als je die ook met elkaar deelt. Want zo'n lange reeks van karakters is niet makkelijk te vergelijken op twee beeldschermen.

**Opdracht 10.** Op Were Di gebruiken we een RAID 5 backup systeem. Dit systeem is geplaatst in een ander gebouw dan de werkende (productie)servers. De clouddata (zoals OneDrive, Outlook en Teams) is opgeslagen op een server in Amsterdam.

**Opdracht 11.** De school zou het beste nog een kopie kunnen opslaan op een andere locatie. Breekt er brand uit, dan raakt de school alle gegevens kwijt.

**Opdracht 12.** -

## 6.2 Bedreigingen

**Opdracht 1.** Let's Encrypt is een populaire instantie die certificaten voor HTTPS uitdeelt, omdat Let's Encrypt dat als enige partij gratis doet. Bekijk de pagina met uitleg <https://letsencrypt.org/docs/challenge-types/>. Op welke manieren kun je bewijzen dat een website van jou is? Antwoord steeds 'ja' of 'nee'.

- (a) Ja.
- (b) Nee.
- (c) Ja.

Met de HTTP-01 challenge kun je een bestand op je website zetten. Een brief sturen heeft geen zin. Met de DNS-01 challenge kun je een DNS-record aanmaken. Er bestaan verschillende programma's die dit allemaal automatisch doen.

**Opdracht 2.**

- (a) Het certificaat is uitgegeven door QuoVadis PKIOverheid Server CA 2020.
- (b) In deze lijst vind je Government of The Netherlands, PKIOverheid (Logius). Logius is onderdeel van het ministerie van Binnenlandse Zaken en geeft onder andere certificaten uit voor overheidswebsites.

**Opdracht 3.** C. In tegenstelling tot sommige andere berichten-apps gebruikt WhatsApp end-to-end encryptie om er zeker van te zijn dat je communiceert met de persoon met wie je denkt te communiceren. En dat er niemand tussen jullie in is, zelfs WhatsApp niet. Berichten zijn versleuteld met een slot, en alleen de

ontvanger en jij hebben de sleutel om het bericht te ontsleutelen. Voor extra veiligheid wordt ieder bericht automatisch versleuteld met een andere sleutel en slot.

**Opdracht 4.** Alleen d en f zijn goed.

Wachtwoorden a en b liggen voor de hand en zullen binnen no-time geraden worden. Wachtwoord c bevat de naam van de website en een voornaam. Wachtwoord d is zo complex dat het een paar miljoen jaar zal duren om het te kraken. Wachtwoord e is willekeurig, maar niet complex: het bevat alleen kleine letters. Daarmee is het wachtwoord binnen een paar seconden geraden. Wachtwoord f bevat woorden uit het woordenboek, maar is enorm lang. Ook is Leet Speak (het vervangen van letters door cijfers) gebruikt om het wachtwoord ingewikkelder te maken.

**Opdracht 5.** 123456, password en abc123 komen ieder jaar voor.

**Opdracht 6.** Vaak herken je een phishingmail aan taal- en stijlfouten. Ook is het belangrijk om naar het e-mailadres van de afzender te kijken.

**Opdracht 7.**

- Het is ongebruikelijk dat er in officiële e-mails gewisseld wordt in de aanspreekvorm ('jij' en 'u').
- Het feit dat de klant niet bij naam genoemd wordt is verdacht.
- Het feit dat er ingelogd moet worden via een link is verdacht. Een bedrijf als ING zou normaliter verwijzen naar de website of de app en zou geen link in de mail zelf plaatsen.

**Opdracht 8.** Hopelijk had je ze allemaal goed. Maar het gaat erom dat je ook bij de foute antwoorden wat hebt geleerd.

**Opdracht 9.** B en C. Een trojan horse is de enige malware die pas actief wordt als de gebruiker het opent.

**Opdracht 10.** A en B. Een virus is geen computerprogramma, maar besmet bestaande software.

**Opdracht 11.** A en C. Shareware bevat meestal ook adware, om op een legale manier reclame te maken.

**Opdracht 12.** A, B en C. Alle drie de soorten installeren zich op een systeem. Spyware en adware doen dat echter ongemerkt en richten daarbij geen directe schade aan.

**Opdracht 13.** C. Spyware en adware maken een systeem hooguit trager. Ransomware versleutelt bestanden, zodat je niet meer verder kunt werken.

**Opdracht 14.** Bijvoorbeeld de ransomware DoubleLocker, dat verspreid wordt via gehackte websites. Het versleutelt al je bestanden en verandert je pincode. Daarna vraagt het ongeveer 45 euro om weer toegang te krijgen. Je kunt die betalen met Bitcoins. Als je niet wilt betalen, kun je je telefoon terugzetten naar de fabrieksinstellingen. Je bent dan wel al je gegevens kwijt, behalve als je een backup hebt gemaakt. Bron: <https://www.rtlnieuws.nl/technieuws/nieuwe-android-ransomware-verandert-je-pincode>



### 6.3 Aanvallers en verdedigers

**Opdracht 1.** Gevoelige data, zoals persoonlijke informatie of foto's, staan waarschijnlijk op je smartphone of op een social-media-account. Ook je huisarts heeft misschien wel allerlei informatie over jou.

Je smartphone kan gestolen worden en vervolgens gekraakt. Je social-media-account kan op heel veel manieren worden gehackt. Niet alleen omdat iemand je wachtwoord afkijkt. Maar bijvoorbeeld ook als een hacker toegang krijgt tot de database van het social medium. Je huisarts kan ook gehackt worden. Zeker als hij verouderde software gebruikt.

**Opdracht 2.** B, D en F.

**Opdracht 3.** Voor hacken krijg je maximaal 6 maanden gevangenisstraf of een geldboete van de derde categorie. Steel je vervolgens gegevens, dan wordt het vier jaar gevangenisstraf of een geldboete van de vierde categorie.

**Opdracht 4.** Bijvoorbeeld de responsible disclosure van Thuisbezorgd.

- (a) Kwetsbaarheden in alle Thuisbezorgd-websites en -apps. Een aantal websites is uitgezonderd.
- (b) Dat je een rapport maakt op Bugcrowd.
- (c) De informatie delen met anderen, gegevens inzien of aanpassen, Thuisbezorgd uit de lucht halen, social engineering toepassen, brute force toepassen en gevoelige gegevens openbaar maken.
- (d) Afhankelijk van de ernst van het probleem kun je tot 5000 dollar ontvangen.
- (e) Er zijn enkele test-postcodes met restaurants die niet echt bestaan.

**Opdracht 5.** B.

**Opdracht 6.** B. Je kunt het manifest hier vinden: <https://www.indybay.org/newsitems/2010/12/09/18666107.php>.

**Opdracht 7.** Bijvoorbeeld: Anonymous hackte de Russische staatstelevisie en zond daarop (verboden) beelden uit van de oorlog met Oekraïne. (<https://nypost.com/2022/03/07/anonymous-hacks-russian-state-tv-with-footage-of-ukraine-war/>)

**Opdracht 8.** -

### 6.4 Maatregelen

**Opdracht 1.** Vaak staan de links naar de privacy-informatie in de footer, onderaan de pagina.

**Opdracht 2.**

- (a) juist.
- (b) onjuist.

*Het datalek had voorkomen kunnen worden, door het ID-nummer niet op te nemen in de URL. Dat heeft niet met verouderde software te maken, maar met de wijze waarop gegevens wel of niet openbaar zijn (in dit geval in de URL).*

**Opdracht 3.** *Hopelijk voor je is het bestand veilig. Als dat niet zo is, kun je het bestand het beste direct verwijderen van je computer (dus ook uit de prullenbak).*

**Opdracht 4.**

(a) juist.

(b) onjuist.

*De website is uit de lucht gehaald en wordt geheel opnieuw ontwikkeld. Er worden dus geen maatregelen getroffen in de bestaande website. Een ander datalek is voorkomen voordat de website online ging.*

**Opdracht 5.** B, E en F.

*Correctie en repressie hebben te maken met de hard- en software zelf. Het informeren van klanten (B) valt daar niet onder. E en F zijn preventie.*

**Opdracht 6.** C

**Opdracht 7.** A

**Opdracht 8.** B, D en E.

**Opdracht 9.** *Beantwoord onderstaande vragen over public key encryptie met ja of nee.*

(a) Ja. Eve weet ook de public key.

(b) Nee. Bob moet de public key genereren.

(c) Nee. Alice kent de private key niet.

**Opdracht 10.** *Eigen antwoord.*

(a) *Misschien heb je ooit per ongeluk een besmet bestand (malware) geïnstalleerd of is je social media-account gehackt.*

(b) *Mogelijk heb je de malware verwijderd / een systeemherstel toegepast. De hack kan zijn opgelost door een melding bij de moderator van het social medium of door het wachtwoord te wijzigen.*

(c) *Hopelijk let je nu beter op de beveiliging van je apparaten en ben je alerter op malware. Ook ga je misschien gebruikmaken van sterke antivirus- en malwareprogramma's. Tevens heb je hopelijk geleerd sterke wachtwoorden te kiezen of deze nooit af te geven, ook niet aan vrienden of klasgenoten. Zij kunnen het wachtwoord namelijk ook doorspelen en hun apparaat kan ook gehackt worden, waarna de dader toegang heeft tot jouw wachtwoorden.*

**Opdracht 11.** *Hopelijk allemaal.*

**Opdracht 12.** *Hopelijk allemaal.*