**Samenvatting**

Inhoud

**Hoofdstuk 2: Data, beveiliging en datalek**

[Gouden regels in data protection 4](#_Toc29151897)

[Data breaches 4](#_Toc29151898)

[Gegevens 4](#_Toc29151899)

[Mogelijke oorzaken 5](#_Toc29151900)

[Mogelijke gevolgen 5](#_Toc29151901)

[Beveiligen 5](#_Toc29151902)

[Ashley Madison 5](#_Toc29151903)

[Never forget 6](#_Toc29151904)

[Inhoud security 6](#_Toc29151905)

[Domeinen 6](#_Toc29151906)

[CIA-driehoek 7](#_Toc29151907)

[Hosting 7](#_Toc29151908)

Hoofdstuk 3: Threats and protection

[Malware 8](#_Toc29151909)

[Threats 8](#_Toc29151910)

[*1) Malware: computer virus 8*](#_Toc29151911)

[*2) Malware: ransomware, trojan horse, worms 10*](#_Toc29151912)

[*3) Andere malware 11*](#_Toc29151913)

[*4) Hacking en cracking 12*](#_Toc29151914)

[*5) Slechte beveiliging 13*](#_Toc29151915)

[Protection 14](#_Toc29151916)

[*1) Antivirus en antimalware 14*](#_Toc29151917)

[*2) Firewall 14*](#_Toc29151918)

[*3) Doeltreffende wachtwoorden 14*](#_Toc29151919)

[*4) Back-up 15*](#_Toc29151920)

[*5) Awareness 16*](#_Toc29151921)

Hoofdstuk 4: Wireless communication

[Termen 16](#_Toc29151922)

[Router 16](#_Toc29151923)

[Switch 16](#_Toc29151924)

[Wifi heat map 16](#_Toc29151925)

[IEEE 802x 17](#_Toc29151926)

[WPS 17](#_Toc29151927)

[WEP 17](#_Toc29151928)

[WPA 17](#_Toc29151929)

[WPA2 17](#_Toc29151930)

[SSID 18](#_Toc29151931)

[ESSID 18](#_Toc29151932)

Hoofdstuk 5: Security audit

[Security audits 18](#_Toc29151933)

[Security audit categorieën 18](#_Toc29151934)

[Voorbereiding audit 19](#_Toc29151935)

[Audit uitvoeren 20](#_Toc29151936)

[*1) Audit questionnaire 20*](#_Toc29151937)

[*2) Audit obligations 22*](#_Toc29151938)

Hoofdstuk 6: Wetgeving

[Wat moet je kennen en kunnen in dit hoofdstuk? 22](#_Toc29151939)

[GDPR 22](#_Toc29151940)

[Wat? 22](#_Toc29151941)

[Inhoud? 22](#_Toc29151942)

[Nut? 23](#_Toc29151943)

[Voordelen voor bedrijven 23](#_Toc29151944)

[Verplichtingen voor bedrijven (en dus ook verwerkers) 24](#_Toc29151945)

[Basisprincipes voor bedrijven 24](#_Toc29151946)

[*1) Het beginsel van rechtmatigheid, behoorlijkheid en transparantie 24*](#_Toc29151947)

[*2) Het beginsel van de doelbinding 24*](#_Toc29151948)

[*3) Het beginsel van de minimale gegevensverwerking 25*](#_Toc29151949)

[*4) Het juistheidsbeginsel 25*](#_Toc29151950)

[*5) Het beginsel van de beperkte bewaartermijn 25*](#_Toc29151951)

[*6) Het integriteits- en vertrouwelijkheidsbeginsel 25*](#_Toc29151952)

[Register van de verwerkingsactiviteiten 25](#_Toc29151953)

[Grootschalige datawerking 26](#_Toc29151954)

[Gegevenslek 26](#_Toc29151955)

[Rechten van een individu: 27](#_Toc29151956)

[Beroep aantekenen: 29](#_Toc29151957)

[Inperken van rechten? 30](#_Toc29151958)

[Rechten uitoefenen: 31](#_Toc29151959)

[DPO 32](#_Toc29151960)

[Gegevensbeschermingseffectbeoordeling (GEB) 33](#_Toc29151961)

Hoofdstuk 7: Hacking

[Wat mag je hacken? 34](#_Toc29151962)

[Wetgeving 34](#_Toc29151963)

[Hackers-platform 35](#_Toc29151964)

[SQL injection 35](#_Toc29151965)

[Wat? 35](#_Toc29151966)

[Welke SQL-producten 35](#_Toc29151967)

[Welke kennis 35](#_Toc29151968)

[Countermeasures 36](#_Toc29151969)

**Hoofdstuk 2: Data, beveiliging en datalek**

# Gouden regels in data protection

Een goede voorbereiding is essentieel voor data protection. Ga nooit ad hoc beveiligen en zorg ervoor dat je altijd een strak plan hebt. Een goed voorbeeld hiervan is een security audit. Daarnaast is het heel belangrijk dat je je boerenverstand gebruikt: wat je niet in real life doet mag je ook niet digitaal doen. Tot slot is het belangrijk dat je de wetgeving kent zodat je weet wat je doet. Deze wetgeving stelt dat je beveiliging steeds in verhouding moet staan tot de soort data (persoonlijke- en openbare gegevens) en de eigen middelen. Ook je basisbeveiliging moet in orde zijn (fysieke beveiliging, antimalware, …

# Data breaches

*Een data breach of datalek is het intentioneel/ onintentioneel loslaten van beveiligde of privé/ confidentiële informatie aan een omgeving die niet vertrouwd wordt met deze data. Dit kan gebeuren door hackers maar ook per ongeluk door een bedrijf zelf.*

## Gegevens

Gegevens of data zijn, da dag van vandaag, heel nuttig. Je kan ze op verscheidene manieren gebruiken. Een heel goed voorbeeld hiervan is reclame maken. We onderscheiden twee soorten gegevens: persoonlijke data en data. Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde- of een identificeerbare, levende, natuurlijke persoon. Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens. Ook persoonsgegevens waarbij de identiteitsgegevens zijn verwijderd, versleuteld, of gepseudonimiseerd zijn persoonsgegevens. Voorbeelden van dingen die persoonsgegevens zijn versus voorbeelden van data zijn:

|  |  |
| --- | --- |
| **Persoonlijke data** | **Data** |
| * Telefoonnummer * Naam * Adres * Geboortedatum * Data | * Design/ bouwplan van een elektrisch toestel * Aankooplijst speelmateriaal jeugdbeweging |

Er is dus een hele grote verscheidenheid aan gegevens en die kan je best beschermen. Je wilt immers niet dat iedereen alles over je te weten komt, toch?

## Mogelijke oorzaken

Een datalek kan diverse oorzaken kennen:

|  |
| --- |
| **Hackers** die bewust netwerken aanvallen om data te **stelen**. |
| **Interne, ontevreden medewerkers** die **gegevens** van het netwerk **kopiëren**. |
| **Technische problemen** waardoor gegevens onbedoeld vrijgegeven worden. |
| **Malware**, zoals virussen, die gegevens naar een malafide webserver doorsturen. |
| **Menselijke fouten**, zoals het ter goeder trouw doorgeven van gegevens aan niet-geautoriseerde personen. |
| … |

## Mogelijke gevolgen

Data breaches passeren soms ongezien maar ze kunnen toch zeer ingrijpende gevolgen hebben. Dit zijn mogelijke gevolgen van een datalek:

|  |
| --- |
| Financiële schade |
| Imagoschade |
| Operationele problemen |
| Boetes |
| Persoonlijke schade |
| … |

## Beveiligen

Om een data breach te voorkomen moet je je data beveiligen. De te beschermen data kan je opdelen in drie categorieën:

|  |
| --- |
| **Persoonlijke** data (bv: medisch dossier, gezinssamenstelling, …) |
| **Bedrijfsgegevens** (bv: productplannen, work flows, …) |
| Gegevens van **verenigingen** (bv: leden, budget, …) |

Je kan op twee manieren beveiligen: analoog en digitaal. Analoge beveiliging is beveiliging die je uitvoert in de echte wereld. Een voorbeeld van analoge beveiliging is een contract persoonlijk bezorgen aan de medecontractant om te voorkomen dat het kwijt raakt, gestolen wordt of onderschept wordt. Digitaal beveiligen kan je doen door een firewall, encryptie, back-ups, … Dit doe je dus op digitaal niveau.

## Ashley Madison

Ashley Madison is een goed voorbeeld van hoe schadelijk de gevolgen van een data breach kunnen zijn. De site was een dating site voor al getrouwde partners om een minnaar/ minnares te vinden en het was dus niet de bedoeling dat de partners van de leden erachter zouden komen dat zij vreemd gingen. Het lekken van de namen van hun leden had dus zware gevolgen voor de leden. Hieruit kan je de wijze les trekken dat je jezelf altijd moet afvragen wat de gevolgen zijn als je gegevens in een data breach terechtkomen.

## Never forget

Het is belangrijk dat je de wetgeving rond data goed kent en dat je daarnaast ook voorbereid bent op een data breach. Dit is omdat de vraag niet is of je een data breach gaat hebben maar wanneer. Daarom kan je best het volgende doen:

|  |
| --- |
| Stel een **disaster team** samen met **taken en contactgegevens.** |
| Laat het disaster team **regelmatig samenwerken** zodat zij voorbereid zijn in het geval van een data breach. |
| Bereid een **noodplan** voor. Dit plan kan **deeltaken** bevatten zoals perscommunicatie al voorbereiden, schadevergoedingsbudgetten, … |

**Hoofdstuk 3: Threats and protection**

# Inhoud security

## Domeinen

* *Netwerkbeheer:*

|  |
| --- |
| Routers |
| Switches |
| Firewall[[1]](#footnote-1) |

* *Penetration testing:*

Dit is wanneer je de veiligheid van een systeem (zowel softwaregewijs als hardwaregewijs) test door zelf te proberen er binnen te dringen. Dit valt onder “ethical” hacking.

* *Cryptografie*:

Cryptografie is de techniek van het beveiligen van informatie en communicatie door middel van codes die alleen kunnen vertaald worden door de persoon voor wie deze informatie bestemd is. (crypt = hidden, graphy = writing)

* *SAD =* ***S****ecurity* ***A****rchitecture and* ***D****esign:*

SAD kijkt naar hoe information security controls en safeguards zijn geïmplementeerd in IT-systemen met het doel om aan de principes van de CIA-driehoek te voldoen van de data die gebruikt, geprocessed en opgeslagen wordt in de desbetreffende IT-systemen.

* *(I)SOC =* ***I****nformation* ***S****ecurity* ***O****peration* ***C****enter:*

Een ISOC is een gecentraliseerde unit die zorgt voor de veiligheidsproblemen op een organisatorisch en technisch level. Een ISOC gebruikt data processing technologie.

* *Fysieke beveiliging*
* *Toegangscontrole (door bijvoorbeeld IAM[[2]](#footnote-2))*
* *Wetten (gecontroleerd door een DPO[[3]](#footnote-3))*
* *GRC =* ***G****overnance,* ***R****isk and* ***C****ompliance:*

GRC houdt de maatregelen in die een bedrijf heeft voor de drie velden om te voorkomen dat er iets mis gaat en om de situatie op te lossen wanneer er iets misgaat (het is geen kwestie van OF er iets misgaat maar WANNEER). Dit houdt dus ook in dat de risico’s in kaart worden gebracht.

* *BC =* ***B****usiness* ***C****ontinuity:*

Dit zijn maatregelen die een bedrijf neemt om te verzekeren dat het bedrijf niet volledig stilligt als er iets gebeurt maar nog steeds zo goed mogelijk kan functioneren.

* *DRP =* ***D****isaster* ***R****ecovery* ***P****lanning:*

Dit is een gedocumenteerd proces of een set van procedures die doorlopen worden als er iets misgaat om ervoor te zorgen dat de gevolgen zo klein mogelijk zijn bij hacking, data breaches, …

## CIA-driehoek

Deze driehoek is de basis voor information security en beveiligingsmaatregelen rond IT-gerelateerde zaken. Het doel is om de CIA te waarborgen. CIA staat voor:

1. *Confidentialtity:* De gegevens zijn vertrouwelijk en enkel de nodige gegevens mogen opgezocht worden door personen die hiertoe bevoegd zijn of recht hebben op deze gegevens.
2. *Integrity:* De gegevens zijn correct en volledig.
3. *Availability:* De gegevens zijn beschikbaar voor iedereen die daar recht op heeft.

Een aantal voorbeelden van een schending van de CIA-driehoek zijn:

|  |
| --- |
| Een agent controleert het vervallen van de groene verzekeringskaart van een chauffeur na een aanrijding. |
| Een agent controleert het vriendje van zijn dochter in de polititedatabase. |

## Hosting

Er zijn verschillende soorten hosting met elk hun eigen eigenschappen. Dit zijn drie voorbeelden van hosting:

|  |
| --- |
| **Shared hosting:**  Dit is wanneer je je **app, webshop, website** op het internet zet. Deze zijn **licht** dus kan je er **meerdere op één server** zetten. Dit is gevaarlijk voor hackers want als de **hackers** de server hebben gehackt kunnen zij **aan alles** wat erop staat. |
| **Dedicated hosting:**  Dit is wanneer je iets host met maar **1 admin** (deze is dus geldig voor 1 klant). Dit betekent dat **alle hardware van jou** is en dit kan enkel **gereset** worden door **jezelf**. |
| **Virtual private hosting:**  Dit is een **combinatie** van dedicated hosting en shared hosting. Hierbij heb je **4 à 5 virtuele users** die hun **eigen toestellen volledig zelf kunnen installeren**. Doordat de **hardware gedeeld** is, is de **kostprijs ook gedeeld**. Als iemand een reset doet, krijgt **iedereen** een **reset.** |

# Malware

*Malware is een verzamelnaam voor software die tot doel heeft om schade toe te brengen aan computersystemen.*

## Threats

### Malware: computer virus

Een virus[[4]](#footnote-4) is een vorm van malware. Het is een computerprogramma dat zichzelf in een bestand kan nestelen (zoals in de bestanden van je besturingssysteem). Virussen kunnen de computer trager maken, schade aanrichten (zoals het wissen of verspreiden van gevoelige gegevens) of de controle van de computer overnemen. Het is de bedoeling dat een virus zo klein mogelijk is want dit is makkelijker te verspreiden. Symptomen van een virus kunnen zijn:

|  |
| --- |
| **Ongewone** **pop-ups** of vreemde pop-ups |
| Plotse **performanceproblemen** |
| **Verdachte harde-schijfactiviteit** |
| Onverwacht **gebrek aan opslagruimte** |
| **Ontbrekende** (systeem-)**bestanden** |
| De **home-page** van je **web browser** is plots **veranderd** |

Virussen op je computer kunnen ontdekt worden aan de hand van twee technieken:

|  |
| --- |
| **Signatures:**  Dit is de spreekwoordelijke “**vingerafdruk[[5]](#footnote-5)**” van een virus. Het is een **set** van **unieke data** of **stukjes code** die ervoor zorgen dat je antimalware het virus kan **identificeren**. Je antimalware definieert deze “vingerafdruk” als een “**definition file**” oftewel een DAT-file. |
| **Heuristics:**  Dit is een manier om **problemen op te lossen** met behulp van een **praktische methode** die **niet gegarandeerd** is om de **perfecte oplossing** te vinden maar die wel voldoende is om het probleem **snel** op te lossen. In computers wordt dit gedaan door het **gedrag van een programma na te doen** door bestanden te openen, er code aan toe te voegen en zichzelf te kopiëren. |

We kunnen virussen classificeren op basis van het infectietype en het gedrag:

|  |
| --- |
| **Armoured virus:**  Dit is een virus met een **heel ingewikkelde code** zodat er tijd voor nodig is om het virus te ontcijferen of het virus **verbergt zijn echte locatie** voor de antimalware. |
| **Boot sector virus:**  Dit is een virus dat de **Master Boot Record** **infecteert**. Het wordt **actief** **voor** het **besturingssysteem** opgestart wordt. Dit heeft tot het gevolg dat de **antivirus** het virus **niet kan vinden** eenmaal het op je computer staat. Het **verplaatst zich** wanneer de antivirus een bepaalde plaats scant. Dit is hetzelfde als een MBR-virus. |
| **File erase:**  Dit virus **verwijdert** cruciale **OS-bestanden** en/ of **databestanden**. |
| **Ghost virus:**  Dit is een virus dat je kan te pakken krijgen als je je **antivirusprogramma** **tussen** je **bios** en **OS** zetten door middel van een **USB-stick.** |
| **Hybrid virus:**  Dit virus **combineert** verschillende kenmerken/ acties van andere virussen. |
| **Macro:**  Een macro zijn **scripts** die in een **scripttaal** geschreven zijn. |
| **Mass mailer:**  Dit is malware die zich **vermenigvuldigt** in de vorm van een **e-mail attachment** en het **adresboek van de geïnfecteerde** gebruikt om zo het virus **door te sturen** naar weer een nieuw persoon. |
| **Polymorphic virus:**  Dit virus verandert door **encryptie** zijn eigen code bij een **kopieeractie**. Het virus **kopieert zichzelf** constant om niet ontdekt te worden. |
| **Retro virus:**  Dit is een virus dat de **antivirussoftware** en/ of de **firewall** **stopt** en/ of de **virusdatabase** **verwijdert**. |
| **Stealth virus:**  Dit virus **verbergt** zichzelf door de **bestandsgrootte** **aan te passen** en/ of de **directory**. |

Een beter woord voor virus zou eigenlijk infector kunnen zijn aangezien het programma schone bestanden infecteert (door code aan het bestand toe te voegen). Je kan ze indelen in vier categorieën:

|  |
| --- |
| **Macro virussen:**  Programma’s zoals Microsoft **Word** en **Excel** werken met een **macroscriptingtaal**. Een **kwaadwillig script** dat zich bijvoorbeeld in een **template** **verstopt** kan voor schade zorgen. Een voorbeeld hiervan is het toevoegen van wachtwoordbeveiliging aan een document, het verwisselen van woorden, het toevoegen van tekst, het wijzigen van berekeningen, … |
| **File infectors:**  Dit zijn virussen die **bestanden** **wijzigen** door bijvoorbeeld het toevoegen van code, het wijzigen van inhoud, … |
| **System infectors:**  Dit zijn virussen die het **besturingssysteem aantasten** door bijvoorbeeld systeembestanden te verwijderen, DLL’s veranderen, … |
| **Boot record infectors:**  Dit zijn virussen die zich op de **MBR** vestigen. Daardoor worden ze **actief voor** het **besturingssysteem** en in principe dus ook voor het **laden van de virusscanner** en kunnen ze de **virusscanner manipuleren** (bijvoorbeeld door zichzelf naar een **veilige record** te verhuizen op het moment dat de virusscanner de MBR onderzoekt, om daarna **terug** te gaan naar de MBR). |

Soms kunnen virussen dezelfde namen en/ of eigenschappen vertonen. Wanneer dit voorkomt worden de virussen ondergebracht in families en subfamilies.

### Malware: ransomware, trojan horse, worms

Malware is een samentrekking van malicious software. Het is software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het gaat hier altijd over kwade opzet. Een virus kan malware zijn maar malware hoeft geen virus te zijn. Voorbeelden van malware (die geen virussen zijn) zijn:

|  |
| --- |
| **Ransomware:**  Ransomware is malware die je **gegevens versleutelt**. Meestal vragen hackers na het versleutelen van je gegevens een **vergoeding** om ze terug te ontsleutelen. Het belangrijkste is om de **stroom meteen uit te schakelen** als je merkt dat je hierdoor besmet bent. |
| **Trojan horse/ Trojaans paard:**  Dit is een virus dat zich **vermomt** **als echte** (en normaal gezien onschuldige) **software**. Dit is voor hackers en cyber-criminelen een manier om toegang te krijgen tot systemen. De **schade** is afhankelijk van het **paard**. |
| **Worms:**  Dit is een type van malware dat **kopieën van zichzelf verspreid**t van computer tot computer. Wormen kunnen zichzelf dupliceren zonder menselijke tussenkomst en ze **hoeven niet bevestigd te zijn** aan een softwareprogramma om schade aan te richten. |

### Andere malware

|  |
| --- |
| **Adware:**  Dit zijn **softwareapplicaties** die **advertenties** weergeven terwijl ze draaien. Ook **verzamelen deze gegevens** over wat de gebruiker doet en geeft op basis hiervan bepaalde advertenties weer. Dit is niet toegestaan wanneer er **geen consent** voor gegeven is. |
| **Backdoor:**  Backdoors kunnen door hackers gebruikt worden. Rootkits zetten een **bepaalde poort** op je pc open waardoor hackers dan **binnen kunnen**. Dit is **low-profile**. Aan de hand van backdoors kunnen hackers bijvoorbeeld DDOS-aanvallen[[6]](#footnote-6) uitvoeren. |
| **Bots:**  Bots kan je opsplitsen in **goede en slechte bots** (hoewel er over het algemeen vooral slechte bots zijn). Hun **doel** kan **variëren**. Een bot met **slechte bedoelingen** wordt een **botnet** genoemd. |
| **Dialler:**  Deze malware verbindt een **telefoonlijn** automatisch met een **dure betaallijn.** |
| **Hoaxes:**  Een hoax is een **vals bericht**. Zo kan het zijn dat je een viruswaarschuwing krijgt die natuurlijk niet echt is. Deze waarschuwingen kunnen gebruikt worden op **verschillende manieren.** |
| **Keylogger:**  Deze malware **bewaart** alle **toetsaanslagen** die je doet, je **muisbewegingen** en je **schermoutput**. |
| **Phising:**  Phising is een vorm van **internetfraude**. De opzet is het lokken van nietsvermoedende gebruikers naar een **valse website** die een kopie is van de echte website. Hier wordt er dan geprobeerd om de gebruiker zich **in te laten loggen** met hun inlognaam, wachtwoord of hun creditcardnummer. De sms-variant van dit fenomeen heet **smishing**. |
| **Rogueware:**  Deze malware doet zich voor als beveiligingssoftware en maakt de gebruiker met **valse probleemmeldingen** bang en **stelt voor** om de problemen **op te lossen**. |
| **Rootkit:**  Een rootkit is een **verzameling van programma’s** die zich in het **besturingssysteem** nestelen. Dit kan op **twee niveaus**. Het pakket kan zich op het niveau van de **kernel**[[7]](#footnote-7) ophouden. Dit heeft tot gevolg dat ze **onbeperkt toegang** krijgen tot het **RAM-geheugen** (ook swap-bestanden) en dat ze het **volledige geheugen** van de computer kunnen uitlezen, kopiëren, wijzigen, … Daarnaast zijn er rootkits op **gebruikersniveau**. Zij zorgen voor een **beperkte geheugentoegang** (dit is bij de segmenten die door het besturingssysteem aan de applicaties toegekend zijn). Een rootkit kan je **bijna niet verwijderen** zonder je **besturingssyteem** te **beschadigen.** |
| **Spyware:**  Spyware zijn **computerprogramma’s** die **persoonlijke gegevens verzamelen** en deze **doorsturen** naar een externe partij. Meestal is het doel van spyware het **verdienen van geld** maar dit is **niet altijd** het geval. |

### Hacking en cracking

Zowel hackers als crackers proberen om ongeautoriseerd toegang te krijgen tot data in een computersysteem. Een hacker bouwt rapporten over beveiligingsproblemen terwijl een cracker[[8]](#footnote-8) daadwerkelijk in systemen binnenbreekt. Er zijn verschillende mogelijke hackertypes:

|  |
| --- |
| **White hat[[9]](#footnote-9) hacking:**  Dit wordt ook wel **ethical hacking** genoemd aangezien dit hacking is voor **goede doeleinden** (het zoeken naar zwakke punten om deze op te lossen). Om een white hat hacker te zijn moet je **toestemming** hebben van de **eigenaar** van het computersysteem. |
| **Grey hat hacking:**  Een grey hat hacker hackt **zonder kwade bedoelingen** maar **breekt** wel de **wet**. |
| **Black hat hacking:**  Een black hat hacker is iemand die de **wet breekt** **met kwaadaardige bedoelingen**. Deze staan ook wel bekend als **crackers**. |
| **Red hat hacking:**  Een red hat hacker is een **white hat hacker die een black hat hacker** **bestrijdt** met zijn **eigen wapens.** Deze hacker **rapporteert niet**. |
| **Blue hat hacking:**  Een blue hat hacker is een hacker die hackt als **wraak**. |
| **Green hat hacking:**  Dit is slechts een **beginnende** hacker. |

Naast verschillende hackertypes zijn er ook verschillende crackertypes. Deze zijn:

|  |
| --- |
| **Packet monkeys:**  Deze sturen **grote aantallen van data pakketten** uit om het **netwerkverkeer** **plat** te leggen door een DOS attack te doen. |
| **Script kiddie:**  Dit zijn tieners die met **frameworks[[10]](#footnote-10)** aan de slag gaan **zonder** dat ze **veel** **kennis** hebben. |
| **S’kiddiots:**  Dit zijn **wannabe** hackers die **geen kennis** bezitten. |
| **Black hat hackers:**  Een black hat hacker is iemand die de **wet breekt** **met kwaadaardige bedoelingen**. |

Een hacker hackt in verschillende fases om zo ergens binnen te raken. Dit doet hij als volgt:

|  |
| --- |
| 1. **Informatie verzamelen** 2. **Toegang verwerven** (best tijdens een moment waarop er niemand is) 3. **Toegang behouden** (misschien moet je nog terug komen) 4. **Sporen wissen** (als ze erachter komen dat je er was kan het moeilijker zijn om terug binnen te raken) 5. **Rapporteren** |

Wat een hacker ook kan doen om op een netwerk binnen te raken is social engineering. Dit kunnen ze doen door op de emoties van een werknemer in te spelen met een kleine leugen (bijvoorbeeld: ‘Ik ben mijn wachtwoord kwijt.’). Daarnaast kan een social engineer ook proberen om gegevens te pakken te krijgen door middel van phising of smishing. Ook is het voor hackers interessant om soms de vuilbak te doorzoeken om zo mogelijk nuttige informatie te vinden die is weggegooid. Het is dus belangrijk dat personeel in een bedrijf er zich van bewust is dat deze dingen kunnen gebeuren.

### Slechte beveiliging

Er zijn verschillende types van slechte beveiliging. Dit zijn een aantal types:

|  |
| --- |
| **Fysische problemen:**  Dit kan zijn wanneer de **server room** niet op slot is en dus **vrij toegankelijk** is. Ook de **afwezigheid** van een **UPS**[[11]](#footnote-11) of **firewall** hoort bij deze categorie. **Schade** aan toestellen, technische **mankementen**, het **niet** hebben van **redundante** **toestellen** zijn eveneens mogelijke fysische problemen. |
| **Ontoereikende configuraties** |
| **Onvoldoende back-ups** |
| **Problemen met toegangscontrole:**  Dit kan vrij breed gaan van het **terrein** tot **accounts** op **mobiele apparaten** tot **intranet** en meer. |
| **Verlies van data:**  De verloren data kan gaan van **paswoorden** tot **databases** tot **niet-geautoriseerde shares** en meer. |
| **Vermenging van functies** |

## Protection

### Antivirus en antimalware

Antivirus software heet eigenlijk antimalware. Het doel van deze programma’s is om malware te voorkomen, detecteren en verwijderen. Het programma doet dit door te scannen naar signatures, heuristics, rootkit detection en real-time protection. Het kan echter soms wel voorkomen dat je antimalware een false positive[[12]](#footnote-12) aangeeft en deze in quarantaine zet. Ook is het zo dat real-time protection je systeemprestaties vermindert.

Antimalware zijn echter niet perfect. Zo garandeert geen enkele scanner 100% detectie/ bescherming. Ook is het zo dat nieuwe virussen andere hardware gebruiken (zoals de CPU). Daarnaast kan een virus een geïnfecteerd bestand vinden maar dit bestand kan niet altijd in de oorspronkelijke staat hersteld worden omdat de bestanden reeds beschadigd zijn. Virussen en antimalware kunnen mogelijk ook schrijven in de firmware en wanneer de BIOS geïnfecteerd is kan de antimalware deze niet meer vinden.

Er zijn natuurlijk ook alternatieven voor een antivirusprogramma. Zo kan je bijvoorbeeld gaan voor een UTM[[13]](#footnote-13) of voor een cloud antivirus (deze bieden echter geen bescherming tegen usb-sticks. Online scanners kunnen je dan weer helpen tegen rogueware. Ten slotte heb je ook gespecialiseerde tools die je kunnen helpen in het geval van een infectie.

De kost van een goede veiligheid is echter wel groot maar nog steeds noodzakelijk.

### Firewall

Een firewall is bedoeld om hackers buiten te houden en data binnen het host netwerk. Er zijn twee types van firewalls: hardware firewalls (router provider, WatchGuard, Cisco, Juniper, …) en software firewalls (ZoneAlarm, Comodo, SonicWall VPN, …). Het is zeer belangrijk dat je een firewall correct configureert naar je gebruik.

Een firewall kan op twee niveaus werken: via packet filtering of via application layer filtering. Bij packet filtering kijkt da firewall poortnummer per poortnummer naar en datapakket volgens ingestelde regels. Bij application layer filtering kijkt de firewall ook naar het datapakket zelf en kan zo virussen in het datapakket tegenhouden.

### Doeltreffende wachtwoorden

Een deel van data beveiligen is ook het beveiligen van je wachtwoorden. Daarom is het heel belangrijk dat je een sterk wachtwoord hebt. Zo heeft een sterk wachtwoord een aantal regels:

|  |
| --- |
| Het wachtwoord moet **minimum 12 tekens lang** zijn. |
| Je moet een **combinatie** van **nummers, letters** (zowel hoofd- als kleine letters) en **symbolen** gebruiken. |
| Je kan best **geen** **woordenboekwoorden** of **woordcombinaties** gebruiken. |
| Gebruik **geen** **voor de hand liggende vervangingen** (zoals een ‘o’ vervagen door een ‘0’). |
| Je kan ook kiezen om een **passphrase[[14]](#footnote-14)** te gebruiken. |
| Je kan best gebruik maken van 2FA (= **Two Factor Authentication**). Dit is wanneer je een wachtwoord of pincode hebt maar je hebt ook een **andere controle** die je moet doen om in te loggen. |

Dingen die je best doet om je wachtwoorden te beheren zijn:

|  |
| --- |
| Gebruik **afgekorte zinnen** om je wachtwoord te verzinnen (bijvoorbeeld: iwtf2TM = I want to go to Thomas More). |
| **Wijzig** je wachtwoorden **regelmatig**. |
| **Log** je accounts **volledig uit** in plaats uit in plaats van af te sluiten. |

Er zijn natuurlijk ook dingen die je zeker niet mag doen met je wachtwoord:

|  |
| --- |
| **Sla** je wachtwoord **nooit op in browsers.** |
| Gebruik **hetzelfde wachtwoord** **niet** voor **meerdere accounts.** |
| Gebruik **niet je eigen naam** of die van **kennissen** (gebruik hier ook geen **varianten** op). |
| **Schrijf** je **wachtwoorden** **niet op.** |

Je kan ook gebruik maken van paswoord generators maar deze zijn niet per se betrouwbaar of handig om te onthouden.

### Back-up

*Een back-up of reservekopie is een kopie van gegevens die zich op een gegevensdrager of binnen een applicatie bevinden om deze te kunnen herstellen mochten ze beschadigd raken.*

Het verlies van data kan ernstige gevolgen hebben, daarom is het dus belangrijk dat je back-ups maakt van je data. Er zijn verschillende types van back-ups:

|  |
| --- |
| **Full back-up:**  Dit maakt een back-up van **alle data.** Ook ondersteunt dit encryptie en wachtwoordbeveiliging. Vanuit dit type back-up kan je een incremental of een differential back-up doen. |
| **Incremental back-up:**  Dit maakt een back-up van alle **gewijzigde data** sinds de **laatste back-up.** |
| **Differential back-up:**  Dit maakt een back-up van alle **gewijzigde data** na de **laatste full back-up.** |
| **Mirror back-up:**  Dit maakt een full back-up zonder encryptie of wachtwoordbeveiliging. |

Je kan je back-ups best op een veilige manier bewaren. Zo kan je je tapes in een brandkast leggen die beveiligd is tegen diefstal en brand. Je kan er ook voor kiezen om je data op en aparte locatie te bewaren (waar ze beschermd zijn tegen diefstal en natuurrampen). Ten slotte kan je ervoor kiezen om je back-ups te maken in de cloud die ervoor zorgt dat je data ge-encrypteerd wordt voordat deze het netwerk verlaat.

### Awareness

Awareness is de zwakste schakel in de information security. Dit is omdat gebruikers zich continu bewust moeten zijn van beveiligingsmaatregelen. Dat maakt het dus een taak voor iedereen en niet enkel voor Information Security Officers. Daarom is het belangrijk dat gebruikers regelmatig getraind, gecoached en gemonitord worden.

**Hoofdstuk 4: Wireless communication**

# Termen

## Router

Een router is een apparaat dat twee of meer verschillende computernetwerken aan elkaar verbindt. Een voorbeeld hiervan is internet met een bedrijfsnetwerk. Een router stuurt pakketten data van het ene netwerk naar het andere netwerk. Een router is een schakelapparaat voor datapakketten en wordt beschouwd als een uitvoerapparaat.

## Switch

Een switch is een apparaat in de infrastructuur van pakketgeschakelde[[15]](#footnote-15) computernetwerken dat tot doel heeft toestellen met elkaar te verbinden door het ontvangen, verwerken en doorzenden van ontvangen frames.

## Wifi heat map

Een heat map is een grafische representatie van data waarop de individuele waarden in een matrix zijn opgeslagen als kleuren. Deze map toont de locaties van de sterktes van wifi.

## IEEE 802x

IEEE 802.11 omvat een verzameling van standaarden voor draadloze netwerken. De naam komt doordat deze standaarden ontwikkeld zijn door groep 11 van het IEEE LAN/ MAN standaarden-comité.

## WPS

WPS staat voor **W**ifi **P**rotected **S**etup. Dit is een netwerk security standaard om een veilig wireless thuisnetwerk te creëren. De bedoeling hiervan is ervoor zorgen dat mensen die geen kennis van wireless security hebben toch met hun eigen netwerk kunnen verbinden. Je kan hiermee draadloos verbinding maken zonder dat je een code hoeft te geven.

## WEP

Dit staat voor **W**ired **E**quivalent **P**rivacy. Het is een door de IEEE 802.11 gespecifieerde methode om berichten die via een draadloze verbinding (wifi) worden verstuurd te versleutelen. Het maakt gebruik van de RC4-encryptie van RSA Security. De versleuteling vindt plaats tussen de twee NICs[[16]](#footnote-16) dus deze geldt alleen voor zover de data in de lucht hangt. Zodra de data ontvangen is, is deze niet meer gecodeerd. Om gebruik te maken van WEP moeten de participerende NICs WEP aanzetten en een gelijke sleutel ingevoerd krijgen.

## WPA

Dit staat voor **W**ifi **P**rotected **A**cces. Het is een systeem om veilige draadloze netwerken (wifi) op te zetten. Het is ontwikkeld nadat onderzoekers een aantal zwakke plekken in WEP hadden gevonden. Het is gebaseerd op de IEEE 802.11-standaard en is bedoeld als tussenoplossing voor de problemen met WEP terwijl de nieuwe draadloze veiligheidsstandaard werd ontwikkeld.

De eerste versies gebruikten TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol). Dit zorgde ervoor dat de sleutels regelmatig en automatisch worden gewijzigd. Optioneel kon het ook gebruik maken van AES[[17]](#footnote-17)-technologie. Dit is ondertussen vervangen door WPA2.

## WPA2

WPA2 is verschillend van WPA omdat zij CCMP (**C**ounter **C**ipher **M**ode with **B**lock **C**haining **M**essage **A**uthentication **C**ode **P**rotocol) gebruiken. Dit is gebaseerd op AES (**A**dvanced **E**ncryption **S**tandard). Het gebruik van AES is hier dus niet meer optioneel.

Er was een zwakte ontdekt binnen WPA2 maar de hacker kan die enkel gebruiken als hij binnen het netwerk zit. Een andere zwakte van WPA2 is de optie van WPS die erop zit. Binnen de twee tot 14 uur kan je wifi-netwerk gehackt worden hierdoor. Het beste is dus om je WPS af te zetten op je AP.

## SSID

SSID staat voor **S**ervice **S**et **Id**entifier. Dit is een identificatiemethode die gebruikt wordt in de IEEE 802.11-norm. SSID maakt het mogelijk om draadloze computernetwerken van elkaar te scheiden door elk draadloos netwerk een aparte naam (SSID) te geven. Je kan zelf je naam kiezen.

## ESSID

Dit staat voor **E**xtended **S**ervice **S**et **I**dentifier. Het is de naam van een Acces Point in een netwerk en het groepeert BSSIDs [[18]](#footnote-18)(**B**asic **S**ervice **S**et **I**dentifier).

**Hoofdstuk 5: Security audit**

# Security audits

*Een security audit[[19]](#footnote-19) is een systematische veiligheidsevaluatie van de informatie van een bedrijf door te meten hoe goed het systeem aan de criteria voldoet. Security audits worden vaak gebruikt om de naleving van de regelgeving vast te stellen zodat bedrijven op een correcte manier omgaan met de informatie waar zij over beschikken. Na de audit geeft de auditor aan hoe de zwaktes en mogelijke bedreigingen uitgeschakeld kunnen worden. Ook zijn security audits belangrijk omdat constante updates in de informatietechnologie zorgt voor zwakke schakels in het systeem.*

## Security audit categorieën

Bij een security audit gaat een security auditor stap voor stap na of de informatie binnen een omgeving (zoals een bedrijf) veilig is. Een security audit is op basis van een lijst met criteria. Het maakt onderdeel uit van een security diagnosis waarvan vulnerability assassments, een studie van het volledige IT-systeem, penetration testing en aanval op het systeem deel uitmaken. Bij zo’n audit komen er drie onderdelen aan bod:

|  |
| --- |
| **Technologie:**   * **Fysieke toegang** tot gebouwen, devices, autos, … * **Hardware** (netwerk, computers, laptops, tablets, mobiele telefoons, usb devices, ip-telefoons, printers, data centers, ...) * **Software** (beveiligingssoftware, besturingssystemen, dataverwerkers, games, ...) |
| **Processen:**   * **Wettelijke compliance** (GDPR, toegankelijkheid, …) * **Business management** (hoe verloopt de datastroom binnen het bedrijf en er buiten?) * **Security management** (bestaan er al policies, disaster recovery team, roll back procedures, back-upstrategie, ...) * **Risk management** (inschatten van risico's) * **Control frameworks**[[20]](#footnote-20) (wereldwijd erkende norm voor informatiebeveiliging ISO 27001[[21]](#footnote-21)) * **IT-organisatie chart** * **IT-budget** |
| **People:**   * **User practices** * **Social engineering** * **Security awareness** |

## Voorbereiding audit

Een goede audit moet altijd voorbereid worden. Dit doe je in verschillende stappen:

|  |
| --- |
| **Stap 1: De klant in kaart brengen**  In deze stap breng je de **klant in kaart** omdat het belangrijk is dat je weet van wat je exact een audit gaat uitvoeren. De belangrijkste dingen om in een kaart te brengen zijn:   * **Ondernemingsnummer** * **Vestigingen** * **Vestigingsplaats** (adres + vestigingsnummer) 🡪 dit zijn de plaatsen die je moet nakijken * **Visie van het bedrijf** * **Activiteiten** * **Leveranciers** (binnen- en buitenland/ soort) * **Klanten** (binnen- en buitenland/ soort) * **Technologieën** |
| **Stap 2: Eigen middelen**  Na het in kaart brengen van de klant ga je je **eigen middelen** in kaart brengen. De belangrijkste dingen om hier in kaart te brengen zijn:   * **Teamleden** * **Resources** (hardware, software, expertise, …) * **Voorziene periode audit**[[22]](#footnote-22) * **Back-up-periode** (voor wanneer het niet lukt om de audit binnen de voorziene periode te doen) * **Overmachtsclausules**[[23]](#footnote-23) (deze moeten ook in het contract) |
| **Stap 3: Targets**  Hier ga je bekijken **welke gebieden en bedreigingen** je specifiek **moet nakijken** (op vraag van de **klant**). Hier worden dus alle te auditen **domeinen in kaart** gebracht. Deze onderdelen worden in het **contract** verwerkt. Wilt de klant **later** nog **bijkomende domeinen** toevoegen, dan wordt dit in een **contractbijlage** gezet. |
| **Stap 4: Interviews uitzetten**  Hier ga je samen met de klant bepalen **welke persoonsleden** tijdens de audit **geïnterviewd** moeten worden. De geïnterviewde persoonsleden hangen af van wat voor audit je doet en hoe **relevant** deze mensen zijn **ten opzichte van de informatie** die **onderzocht** moet worden. De lijst met geïnterviewde mensen **kan beperkt worden** omwille van **budgettaire redenen** maar dit is **niet gegarandeerd** (veiligheid mag niet mislopen omwille van een beperkt budget). |

## Audit uitvoeren

### Audit questionnaire

Dit is een lijst met vragen zodat de auditor niets over het hoofd ziet.

|  |  |
| --- | --- |
| 1 | Does your firm have **cyber security policies, procedures, and standards** based on **industry standards**? |
| 2 | Does your firm **protect sensitive information** received **from** a **third-party firm** during transmission between the owning third-party as well as other parties with whom that data is shared (i.e. Encryption, SSL/TLS connections)? |
| 3 | Are **all devices** that **store or process** a **third-party** firm's **sensitive** **information** protected from the Internet by a **firewall**? |
| 4 | Does your firm have designated **Cyber-security personnel**? |
| 5 | Does your firm have a **cyber-security user education** and **awareness** program? |
| 6 | Does your firm perform **cyber security audits** by **external 3rd parties** at least **annually**? |
| 7 | Do all devices that **store or process sensitive information** utilize **antimalware** **software** with **current signature files**? |
| 8 | Do **users** that **can** **access** devices that **store** **or** **process sensitive information** have a **unique** **user** **name** and **complex** **password** to access the system? |
| 9 | Do all **devices that store or process sensitive information** at a minimum have **access** **control** that is configured on a least **privilege model** (a person only has access to the data/device that they need)? |
| 10 | Do all **devices** **that store or process sensitive information** at a minimum have **vulnerability** **scanning** performed at least **monthly**? |
| 11 | Are **vulnerabilities** being **remediated** in a **risk based priority** (highest priority vulnerabilities are fixed first)? |
| 12 | Do all **devices that store or process sensitive information** at a minimum have all **unnecessary ports** and **services** **disabled** and the device is **used** **for** **limited** **functions** (ex. A device acting solely as a file server vs. a file server, FTP server, and web server)? |
| 13 | Do all **devices that store or process sensitive information** at a minimum have **patches** **deployed** for **high risk operating system** and **third-party application** **vulnerabilities** within industry **best practices** (i.e. 48 hours) and **medium/low risk** **patches** to be deployed **in <= 30 days**? |
| 14 | Are all **laptop** **devices** that **store sensitive information** **encrypted**? |
| 15 | Do all **mobile** **devices** (e.g. smartphones, tablets) **that store sensitive information** at a minimum have **configuration** **management** provided by a firm owned centrally managed infrastructure including the **ability** to **remote** **wipe** the device? |
| 16 | Do all **mobile** **devices** (e.g. smartphones, tablets) **that store sensitive information** at a minimum have **access** **control** to the device (complex password to access device)? |
| 17 | Does your firm have a **Computer Incident Response Team** (CIRT) with a **formal** **process** to **respond** to **cyber-attacks**? |
| 18 | When you must **share sensitive information** with other companies, do you require those companies to **follow policies**, and **procedures for cyber security** based on **industry standards**? |
| 19 | Does your firm require **2-factor authentication** for **remote** **access** (e.g. token used in addition to a username and password for VPN login)? |
| 20 | Does your firm perform **industry** **standard** **logging** **and** **monitoring** on devices that store or process sensitive information? |
| 21 | Does your firm **control** **web** **access** based on the risk (e.g. reputation, content, and security) of the sites being visited (e.g. Web Proxy Controls)? |
| 22 | Does your firm have **capabilities** of **detecting** **and** **blocking** **malicious** **e-mail** prior to delivery to the end user? |
| 23 | Does your firm **actively** **participate** in a **cyber-intel sharing forum**? (e.g. ISAC, Infraguard) |
| 24 | Does your firm perform **phishing e-mail testing** of its **employees**? |

### Audit obligations

Een security auditor komt zowiezo in aanraking met data van de klant tijdens zijn audit. Rond deze data zijn dus regels opgesteld, zowel wettelijk als moreel.

De wettelijke verplichtingen zijn in alle Europese landen hetzelfde. Zij bestaan namelijk uit de GDPR en de nationale toevoegingen van het land waar de klant zich bevindt.

De ethische verplichtingen steunen op vier pijlers:

|  |
| --- |
| * **Intregrity** (kan iedereen de auditor vertrouwen?) * **Objectivity** (is de auditor beïnvloedbaar?) * **Professional** **competence** (beschikt de auditor over de juiste competenties, kennis, ervaring en tools) * **Confidentiality** (ontbloot de auditor informatie?) |

**Hoofdstuk 6: Wetgeving**

# Wat moet je kennen en kunnen in dit hoofdstuk?

* Weergeven wat GDPR is.
* Weten wat GDPR inhoudt.
* Een bedrijfssituatie kunnen auditen op GDPR compliancy.
* Adviezen geven over hoe de GDPR (beter) toegepast kan worden in een bedrijfssituatie.

# GDPR

*De GDPR is een wettelijk kader dat de regels uittekent voor het verzamelen en verwerken van persoonlijke gegevens van individuen die in de Europese Unie leven.*

## Wat?

* **G**eneral **D**ata **P**rotection **R**egulation
* = een Europese set aan regels om de persoonsgegevens[[24]](#footnote-24) van burgers beter te beschermen (zowel klanten als personeel)
* AVG (**A**lgemene **G**egevens**v**erordening) = de Nederlandse naam (het is dus wel hetzelfde)
* Is enkel van toepassing op de gegevens van levende personen

## Inhoud?

1. Bescherming van persoonlijke data van de Europese burger (sinds mei 2018) op nationaal vlak.
2. Toepasbaar op alle ondernemingen in de EU

|  |
| --- |
| **Maatregelen** nemen tegen **hackers en datalekken** en sterkere **security** |
| **Procedure** voor **dataverzameling en opslag** van persoonlijke gegevens |
| **Toestemming** vragen om gegevens te **verzamelen en gebruiken** |
| Iedereen heeft het recht om **vergeten** te worden[[25]](#footnote-25) |
| **DPO**[[26]](#footnote-26) |

1. GBA

|  |
| --- |
| Stelt dat men een **datalek** moet **melden** **binnen de 72 uur** |
| Geeft **hoge boetes** bij inbreuken op de GDPR (deze zijn wel in verhouding) |
| Doet **inspectie** na een klacht |

## Nut?

* Er is nood aan harmonisatie van de nationale privacywetgevingen binnen Europa (hiervoor waren deze verschillend per land).
* De regels worden aangepast aan de nieuwe digitale realiteit.
* De GDPR/ AVG geeft de burgers meer controle over zijn gegevens.

## Voordelen voor bedrijven

* **Minder** administratieve **lasten en kosten**
* Meer **rechtszekerheid**
* Vrij in te vullen **documentatieplicht**[[27]](#footnote-27)
* **Gelijke regels** voor iedereen, ook in het buitenland, wat de eerlijke concurrentie binnen de EU bevordert
* Gemakkelijker om gegevens te verwerken **over de landsgrenzen** heen
* 1 bevoegde, **toezichthoudende autoriteit**
* **Globale besparing** van 2,3 miljard euro per jaar

## Verplichtingen voor bedrijven (en dus ook verwerkers)

* Accountability: Een bedrijf moet zich kunnen verantwoorden over wat zij met die gegevens doen.
* Rechten van de betrokkenen: De GDPR/ AVG stelt nieuwe rechten in maar houdt ook in dat de al bestaande rechten gevolgd moeten worden.
* Rechtmatigheid van de verwerkingen
* Beveiliging van de verwerking en melding van inbreuken: Bepaalde inbreuken op beveiliging moeten volgens de GDPR/ AVG direct gemeld worden. Een bedrijf heeft dus meldingsplicht.

## Basisprincipes voor bedrijven

### Het beginsel van rechtmatigheid, behoorlijkheid en transparantie

Dit beginsel gaat over het rechtmatig, behoorlijk en transparant verwerken van gegevens ten aanzien van de betrokkene. Dit houdt in dat er gebruik moet gemaakt worden van duidelijke taal. Dit gaat vooral over de informatie rond de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking. Het gaat eveneens over de bijkomende informatie die kan verstrekt worden zodat een gerechtvaardigde en transparante verwerking verzekerd is. De individuen moeten verwittigd worden van de risico’s, regels, garanties en rechten (en hoe ze die moeten uitoefenen) die verband houden met de verwerking van hun gegevens.

### Het beginsel van de doelbinding

Dit houdt in dat persoonsgegevens moeten worden verkregen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Zij mogen niet verder verwerkt worden op een manier die niet in overeenstemming is met deze doeleinden.

Een uitzondering hierop is de verdere verwerking van persoonsgegevens voor archiveringsdoeleinden, openbaar belang, historisch onderzoek, wetenschappelijk onderzoek of voor statische doeleinden. Verder is een uitzondering ook mogelijk als het doel van de verwerking van persoonsgegevens in eenzelfde lijn ligt als het doel waarvoor deze gegevens zijn verzameld. Ook als de betrokkene zijn toestemming heeft gegeven, mogen zijn gegevens verwerkt worden ook al zijn deze niet in overeenstemming met de doeleinden.

Om te kijken of de gegevens mogen herverwerkt worden is het de taak van de verwerkingsverantwoordelijke om dit na te gaan of dit verenigbaar is met het doel waarvoor de gegevens verzameld zijn. Dit moet de verwerkingsverantwoordelijke doen door eerst aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking te voldoen en door dan een verenigbaarheidsoefening uit te voeren. Daarvoor moet hij rekening houden met:

|  |
| --- |
| Het eventueel **verband** tussen de **doeleinden** waarvoor de gegevens **werden** **verkregen** en de **doeleinden** van de **verdere** **verwerking**. |
| De **context** waarin de **gegevens** **werden** **verkregen** (hierbij moet zeker gelet worden op de **relatie** tussen de **betrokkenen** en de **verwerkingsverantwoordelijke**). |
| De **aard** van de **persoonsgegevens** (vooral als de verwerking slaat op **bijzondere** **categorieën** **persoonsgegevens** of **gegevens** inzake **betreffende** **veroordelingen** en **strafrechtelijke** **inbreuken**). |
| De mogelijke **gevolgen** van **verdere** **verwerkingen** voor de **betrokkenen**. |
| Het bestaan van **passende** **waarborgen** (zoals versleuteling of pseudonimisering) |

### Het beginsel van de minimale gegevensverwerking

Dit houdt in dat persoonsgegevens enkel mogen gebruikt worden voor zover ze noodzakelijk zijn voor het doeleinde waarvoor ze worden verwerkt.

### Het juistheidsbeginsel

Dit houdt in dat de gegevens juist moeten zijn. Indien zij niet juist zijn moeten ze bijgewerkt worden. Om dit te waarborgen moeten alle redelijke maatregelen genomen worden ervoor te zorgen dat er geen onnauwkeurige of onvolledige gegevens zijn.

### Het beginsel van de beperkte bewaartermijn

Dit houdt in dat de betrokkene geïdentificeerd kan worden en niet langer bewaard wordt dan noodzakelijk is voor de verwezenlijking van de doeleinden. Dit houdt dus in dat je een bewaartermijn duidelijk moet vaststellen en dat je een mechanisme moet implementeren waarmee je kunt nakijken of de gegevens verwijderd moeten worden.

Een uitzondering hierop is de verdere verwerking van persoonsgegevens voor archiveringsdoeleinden, openbaar belang, historisch onderzoek, wetenschappelijk onderzoek of voor statische doeleinden.

### Het integriteits- en vertrouwelijkheidsbeginsel

De gegevens moeten volgens een afdoend veiligheidsniveau worden verwerkt door gebruik te maken van passende, technische en organisatorische maatregelen. Dit houdt in dat ze beschermd moeten worden tegen iedere niet toegelaten/ onwettige verwerking, verlies, vernietiging of kwaliteitsverlies van gegevens.

## Register van de verwerkingsactiviteiten

De AVG verplicht de verwerkingsverantwoordelijke (of zijn vertegenwoordiger) en de verwerkers om een interne documentatie bij te houden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid worden verricht. Dit register is een overzicht van de verrichte persoonsgegevensverwerkingen en werkt als een manier om deze te identificeren. Het register moet specifieke informatie bevatten over iedere verrichte verwerking:

|  |
| --- |
| **Wie?**   * Vul de **naam** en de **contactgegevens** in van de **verwerkingsverantwoordelijke** (en zijn wettelijke vertegenwoordiger) en van de **functionaris** voor **gegevensbescherming** als u er een moet aanstellen * Stel een **lijst** op van de **werknemers** |
| **Wat?**   * **Identificeer** de **categorieën** **verwerkte** **gegevens** en de **categorieën** **betrokken** **personen**. * **Identificeer** de zogenaamde **gevoelige** **gegevens** zoals de gezondheidsgegevens en gerechtelijke gegevens. |
| **Waarom?**   * **Identificeer** de **doeleinden** waarvoor de gegevens worden **ingezameld**. Er moet een **beschrijving** gebeuren **per** **doeleinde**. |
| **Waar?**   * **Vermeld** de **categorieën** **bestemmelingen** (ook indien ze in derde landen gevestigd zijn) naar **waar** de **gegevens** worden **overgedragen**. * **Vermeld** de **doorgiften** aan een **derde** **land** of **internationale** **organisatie** en **identificeer** het **land** en in voorkomend geval  de **bestaande** **passende** **waarborgen**. |
| **Tot wanneer?**   * Vermeld voor iedere categorie gegevens de **bewaartermijn**. De bewaartermijn moet niet noodzakelijk uitgedrukt worden in aantal dagen, maanden of jaren maar mag ook verwijzen naar de tijd die noodzakelijk is om een concreet project te realiseren. |
| **Hoe?**   * Geef een **algemene** **beschrijving** van de **ingevoerde** **technische** en **organisatorische** **beveiligingsmaatregelen** die garanderen dat het beveiligingsniveau aan het risico is aangepast. |

## Grootschalige datawerking

De AVG definieert niet wat grootschalige dataverwerking is, hij geeft slechts enkele aanwijzingen. Er wordt aanbevolen om de volgende factoren te onderzoeken om te bepalen of een verwerking al dan niet noodzakelijk is:

|  |
| --- |
| Het **aantal** **betrokkenen** in **verhouding** tot een **betrokken** **bevolking**. |
| Het **volume** **gegevens** en de **waaier** van **verschillende** **verwerkte** **gegevens**. |
| De **duur** of de **permanentie** van de **verwerkingsactitiviteit**. |
| De **geografische** **spreiding** van de **verwerkingsactiviteit**. |

## Gegevenslek

1. Wanneer melden?

|  |
| --- |
| Wanneer een gegevenslek kan leiden tot **hoge risico’s voor iemands rechten en vrijheden**, moet de verwerkingsverantwoordelijke de persoon in kwestie onmiddellijk op de hoogte brengen. |

1. Welke informatie moet er in dit bericht staan?

|  |
| --- |
| De **naam en contactgegevens van de functionaris** voor gegevensbescherming of een **ander contactpunt** waar meer informatie kan worden verkregen. |
| De **mogelijke gevolgen** van dit gegevenslek. |
| De **maatregelen** die de verwerkingsverantwoordelijke voorstelt of neemt om het gegevenslek aan te pakken en eventueel ook de maatregelen die hij neemt om de mogelijke nadelige gevolgen van dit lek in te perken. |

1. Wanneer niet melden?

|  |
| --- |
| Als de verwerkingsverantwoordelijke **passende technische en organisatorische beschermingsmaatregelen** heeft genomen en deze maatregelen zijn toegepast op de persoonsgegevens van het gegevenslek, en vooral de maatregelen die de **persoonsgegevens onbegrijpelijk maken voor onbevoegden** (zoals versleuteling). |
| Als de verwerkingsverantwoordelijke achteraf **maatregelen** heeft genomen om ervoor te zorgen dat het hoge risico voor uw rechten en vrijheden waarschijnlijk **niet meer zal voorvallen.** |
| Als de **kennisgeving onevenredige inspanningen** zou vergen. In dat geval komt er in de plaats daarvan een **openbare mededeling** of een soortgelijke maatregel waarbij u even doeltreffend wordt geïnformeerd. |

## Rechten van een individu:

* *Recht van inzage*: Je hebt het recht om te weten (mist je je identiteit bewijst) of de verwerkingsverantwoordelijke je gegevens verwerkt of juist niet. Als hij ze verwerkt heb je recht om deze gegevens in te kijken of je kan zelfs een kopie vragen en bijkomende informatie ontvangen over:

|  |
| --- |
| De **doeleinden** van de verwerking |
| De **categorieën** van persoonsgegevens |
| De **ontvangers of categorieën van** ontvangers aan wie de persoonsgegevens werden of worden verstrekt en meer bepaald de ontvangers gevestigd in het **buitenland** of **internationale organisaties.** |
| De **bewaartermijn** of, als dat niet mogelijk is, de **criteria** ter bepaling van die termijn. |
| Het bestaan van het recht om de verwerkingsverantwoordelijke te vragen uw persoonsgegevens te **verbeteren,** te **wissen**, de verwerking van uw persoonsgegevens te **beperken** of het recht om **bezwaar** te maken tegen die verwerking. |
| Het recht om een **klacht** in te dienen bij een toezichthoudende autoriteit. |
| De **bron** van de gegevens te weten bij een onrechtstreekse inzameling. |
| Het bestaan van een **geautomatiseerde beslissing**, waaronder ook profilering en nuttige informatie over de onderliggende logica ervan. **Hoe belangrijk** deze verwerking van uw gegevens is en welke **gevolgen** dit voor u kan hebben. |

* *Recht van verbetering:* Je hebt het recht om je persoonsgegevens te verbeteren of aan te vullen indien u dit wenst.
* *Recht van wissen:*Je hebt het recht om te vragen om je gegevens te wissen. Het bedrijf moet dit dan doen tenzij je gegevens onder een bepaalde categorie vallen[[28]](#footnote-28). Om je gegevens te verwijderen moet je wel een specifieke procedure volgen, anders is je verzoek niet geldig. Als je het niet eens bent met de afwijzing van je verzoek dan kan je de GBA contacteren of je kan je tot de rechtbank wenden. Je verzoek moet schriftelijk ingediend worden en je moet je identiteit kunnen bewijzen ook moet u duidelijk aangeven wat de (ernstige) reden is dat u wilt dat uw gegevens verwijderd worden.
* *Recht van overdraagbaarheid:*Dit recht zorgt ervoor dat je meer controle hebt over je gegevens. Je kan dit recht in twee gevallen uitoefenen: het moet gaan om een gegevensverwerking die berust op uw toestemming of op een overeenkomst. Dit recht heeft twee aspecten:

|  |
| --- |
| Je hebt het recht om je **persoonsgegevens** die je aan de verwerkingsverantwoordelijke hebt gegeven **terug te krijgen**. |
| Je hebt het recht om uw **gegevens door te geven** aan een **andere verwerkingsverantwoordelijke** of dienstenaanbieder zonder dat de eerste verwerkingsverantwoordelijke, aan wie je de gegevens in de eerste gegevens hebt gegeven, zich daartegen kan verzetten. |

* *Recht van beperkte verwerking:* Als je wilt kan je een beperking krijgen voor het verwerken van je gegevens. Dit houdt in dat de verwerkingsverantwoordelijke enkel nog je gegevens mag opslaan en niet verwerken. Dit kan in vier gevallen gebeuren:

|  |
| --- |
| Je **betwist** de **juistheid van je gegevens**. In dit geval kan de verwerking van je gegevens **beperkt** worden voor de **tijd** die de verwerkingsverantwoordelijke **nodig** heeft om de juistheid na te gaan. |
| Hoewel de **verwerking onrechtmatig** is, wil je **niet dat je gegevens worden gewist** en je eist in de plaats daarvan een beperkt gebruik van gegevens. |
| De verwerkingsverantwoordelijke heeft uw **gegevens niet langer nodig** maar u hebt ze **zelf nog nodig** om uw rechten vast te stellen, uit te oefenen of te verdedigen voor een rechtbank. |
| Je hebt **bezwaar gemaakt tegen de verwerking**. In dat geval kan de gegevensverwerking **beperkt** worden **in afwachting van het antwoord** op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van jou. |

Als je een verwerkingsbeperking hebt verkregen, moet de verwerkingsverantwoordelijke je op de hoogte brengen vooraleer hij die beperking opheft. Men kan uw gegevens niet meer bewerken tenzij er sprake is van deze gevallen:

|  |
| --- |
| Je gaf **toestemming** voor de verwerking. |
| Het gaat om de **instelling, uitoefening of onderbouwing** van een **rechtsvordering**. |
| De **rechten** van een andere **natuurlijke- of rechtspersoon** moeten worden **beschermd**. |
| Er zijn **redenen van zwaarwegend algemeen belang** van de Unie of een lidstaat. |

* *Recht van bezwaar:* Je hebt het recht om bezwaar te maken tegen het feit dat je gegevens worden verwerkt als die verwerking berust op een algemeen belang of het gerechtvaardigd belang van diegene die je gegevens verwerkt. Bovendien kan je je recht van bezwaar laten gelden als je persoonsgegevens worden verwerkt voor directe marketingdoeleinden. Dit recht van bezwaar geldt ook voor profilering die de basis vormt voor verwerkingen voor directe marketingdoeleinden. Er zijn hier geen wettelijke basissen omdat er reeds mechanismen bestaan waarmee hetzelfde doel kan worden bereikt:

|  |
| --- |
| Als de verwerking van je gegevens **gebaseerd is op je toestemming** kan je je toestemming **intrekken**. |
| Als de verwerking van je gegevens **gebaseerd is op een** **overeenkomst**, kan je de **overeenkomst verbreken.** |

Omdat er hier niet langer verwezen wordt naar je specifieke situatie moet je geen specifieke redenen geven voor je bezwaar. Wanneer je bezwaar maakt tegen de verwerking mag de verwerkingsverantwoordelijke je gegevens niet meer verwerken tenzij hij kan bewijzen dat er dwingende, gerechtvaardigde gronden zijn voor die verwerking die zwaarder wegen dan je belangen, rechten en vrijheden of als hij bewijst dat hij ze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Nog twee belangrijke dingen rond het recht van bezwaar:

|  |
| --- |
| De ene heeft te maken met de manier waarop u informatie krijgt: ten laatste **tijdens** uw **eerste contact**, moet het "**algemeen**" recht van bezwaar en het "**direct marketing**" recht van bezwaar uitdrukkelijk, **duidelijk en gescheiden** van overige informatie**, onder je aandacht worden gebracht.** |
| Je mag er bezwaar tegen maken dat je gegevens worden verwerkt voor **wetenschappelijk, historisch of statistisch onderzoek** als dit verband houdt met uw specifieke situatie. |

## Beroep aantekenen:

1. *Het recht om een klacht in te dienen bij een toezichthoudende autoriteit.*

Als je een klacht hebt kan je een administratief of rechterlijk beroep instellen maar je kan ook een klacht indienen. Dit kan je doen in de lidstaat waar je verblijft, waar je je werkplek hebt of waar de beweerde inbreuk is gedaan. De GBA stelt een klachtenformulier op om het je zo makkelijk mogelijk te maken en zij lichten je in over de stand van zaken, uitkomst en de mogelijkheid om in beroep te gaan voor een rechtbank.

1. *Het recht om een doeltreffende voorziening in rechte in te stellen tegen ons, de GBA.*

Men kan een doeltreffende voorziening in rechte stellen wanneer men een bindend juridisch besluit heeft gekregen. Daarnaast kan je een doeltreffende voorziening in rechte stellen als de GBA je klacht niet behandelt of binnen de drie maanden geen informatie geeft over de vooruitgang of uitkomst van uw klacht. Een klacht tegen het GBA is mogelijk in de volgende gevallen:

|  |
| --- |
| Het GBA heeft je klacht **niet** of maar gedeeltelijk **behandeld**. |
| Het GBA heeft je **niet** **ingelicht** over de opvolging van je klacht of over de uitkomst na behandeling van de klacht (**binnen de drie maanden**). |
| Je bent het **niet eens met het juridisch bindend besluit** dat het GBA heeft genomen (Dit kan je enkel doen bij een besluit en niet bij adviezen of aanbevelingen). |

Je kan enkel een klacht tegen het GBA neerleggen voor een Belgische rechtbank.

1. *Het recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of een verwerker.*

Je hebt het recht om een doeltreffende voorziening in rechte te stellen tegen de verwerkingsverantwoordelijk als je meent dat de rechten die het AVG je verleent werden geschonden omdat je persoonsgegevens niet volgens de regels van de AVG werden verwerkt. Je moet iedere procedure tegen de verwerkingsverantwoordelijke aanspannen:

|  |
| --- |
| Bij de **gerechten van de lidstaat** waar de **verwerkingsverantwoordelijke** een vestiging heeft (een vestiging volstaat, het moet niet gaan om de hoofdzetel) |
| Deze procedure kan ook aangespannen worden voor een rechtbank van de **lidstaat waar u gewoonlijk verblijft,** tenzij diegene die uw gegevens verwerkt een overheid is (in dat geval is de bevoegde rechtbank daar waar deze overheid gevestigd is). |

1. *Het recht om via een vertegenwoordiger te handelen.*

Dit is mogelijk maar de regels hierrond zijn wel zeer streng. Je kan jezelf enkel laten vertegenwoordigen door organen, organisaties of verenigingen zonder winstoogmerk. Zij moeten ook aan een aantal voorwaarden voldoen: ze moeten opgericht zijn overeenkomstig het recht van een lidstaat zijn opgericht, ze moeten statutaire doelstellingen hebben die in het publieke belang zijn. Daarnaast moeten ze actief zijn op het gebied van de bescherming van persoonsgegevens. Je kan in twee gevallen jezelf laten vertegenwoordigen:

|  |
| --- |
| **De vertegenwoordiger met je volmacht:**  Je geeft een **volmacht** aan een organisatie zodat deze **in jouw naam een klacht** kan indienen of zodat hij in jouw naam een beroep voor een rechtbank kan instellen tegen de toezichthoudende autoriteit. Ook kan zo’n vertegenwoordiger een beroep instellen voor een rechtbank tegen diegene die jouw gegevens verwerkt. Je kan hem ook een volmacht geven om **in jouw naam het recht op een schadevergoeding uit te oefenen** (dit kan echter enkel als de Belgische wet daarin voorziet wat dus niet het geval is). |
| **De vertegenwoordiger zonder volmacht:**  Het gaat hier om een organisatie die kan handelen **zonder** dat je hen een **volmacht** hebt gegeven. Dit hangt echter volledig af van het optreden van de lidstaten (zij moeten dit soort handeling toestaan en dit moet dus geschreven zijn in het nationaal recht). Indien deze handeling toegestaan is in de lidstaten kan dus een organisatie die voldoet aan de criteria een klacht indienen (hiervoor moet ze geen volmacht van je hebben) wanneer die organisatie van mening is dat je rechten zijn geschonden. Deze organisatie kan ook een **schadevergoeding** vragen **namens de betrokkenen.** (Ook deze mogelijkheid bestaat niet in België) |

## Inperken van rechten?

Soms kunnen je rechter inperken. Dit kan enkel wanneer dit aangegeven is in een Europese of nationale wet. Ook is het noodzakelijk dat deze beperking de essentie eerbiedigt van de fundamentele rechten en vrijheden. Dit zijn mogelijke redenen voor een inperking van de rechten:

|  |
| --- |
| De **nationale veiligheid** |
| **Landsverdediging** |
| De **openbare veiligheid** |
| De voorkoming, het onderzoek, de opsporing en de vervolging van **strafbare feiten** of de **tenuitvoerlegging** van straffen, met inbegrip van de **bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.** |
| Andere belangrijke doelstellingen van **algemeen belang** van de Unie of van een lidstaat, met name een **belangrijk economisch of financieel** belang van de Unie of van een lidstaat, met inbegrip van **monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid.** |
| De **bescherming van de onafhankelijkheid** van de rechter en gerechtelijke procedures. |
| De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de **beroepscodes voor gereglementeerde** beroepen. |
| Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de **uitoefening van het openbaar gezag.** |
| De **bescherming** van de **betrokkene** of van de rechten en vrijheden van **anderen**. |
| De **inning** van **civielrechtelijke vorderingen.** |

Om deze beperkingen beter te kunnen omkaderen, eist de AVG ook dat de wet die uw rechten zal inperken een bepaalde kwaliteit heeft. Ze meten dus bepalingen bevatten die betrekking hebben op:

|  |
| --- |
| De **doeleinden** van de **verwerking** of van de **categorieën** van verwerking. |
| De **categorieën** van **persoonsgegevens**. |
| Het **toepassingsgebied** van de **ingevoerde beperkingen.** |
| De **waarborgen** ter **voorkoming van misbruik** of **onrechtmatige toegang** of **doorgifte**. |
| De **vaststelling** van de **verwerkingsverantwoordelijke** of de **categorieën** van **verwerkingsverantwoordelijken**. |
| De **opslagperiodes** en de **toepasselijke waarborgen,** rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking. |
| De **risico's** voor de rechten en vrijheden van de **betrokkenen**. |
| Het **recht** van betrokkenen om van de **beperking op de hoogte** te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking. |

Ook kan de AVG lidstaten machtigen om te voorzien in bepaalde beperkingen op de rechten van de betrokkenen als het gaat om de vrijheid van meningsuiting, historisch, wetenschappelijk of statistisch onderzoek of archivering in algemeen belang.

## Rechten uitoefenen:

* *Duidelijk*

De verwerkingsverantwoordelijke moet u altijd beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke informatie verstrekken. Die informatie moet in klare en eenvoudige taal opgesteld zijn en aangepast aan de persoon die erom vraagt. De informatie kan schriftelijk meegedeeld worden aar ook mondeling, indien u hierom vraagt.

* *Gratis*

U moet in principe niet betalen voor de informatie die u hebt opgevraagd. Maar als het overduidelijk is dat uw verzoeken ongegrond zijn of overmatig, bijvoorbeeld omdat u steeds hetzelfde opnieuw vraagt, mag diegene die uw gegevens verwerkt ofwel een redelijke vergoeding aanrekenen om zijn administratieve kosten te dekken die hij heeft moeten maken om u de gevraagde informatie te geven of om de maatregelen te treffen waarnaar u hebt gevraagd ofwel het verzoek weigeren. Dit mag enkel mits de verwerkingsverantwoordelijke kan aantonen dat uw verzoek duidelijk ongegrond of overmatig is.

* *Snel*

Zodra u een verzoek doet aan de verwerkingsverantwoordelijke moet deze u op de hoogte brengen van de maatregelen die hij na uw verzoek heeft genomen. Deze informatie moet u binnen de maand, nadat de verwerkingsverantwoordelijke uw verzoek heeft ontvangen, krijgen. Wanneer een verzoek complex is of de verwerkingsverantwoordelijke heeft veel verzoeken te verwerken dan kan het zijn dat deze termijn met 2 maanden wordt verlengd. Echter, wanneer de termijn wordt verlengd, moet de verwerkingsverantwoordelijke u wel op de hoogte brengen en zeggen waarom de termijn wordt verlengd.

* *Voorzichtig*

Als de verwerkingsverantwoordelijke redelijke twijfels heeft over uw identiteit, mag hij u om bijkomende en noodzakelijke informatie vragen zodat hij uw identiteit kan vaststellen. Dit kan u voorkomen door een aantal vormvoorwaarden te eerbiedigen:

|  |
| --- |
| U moet aan de verwerkingsverantwoordelijke een **gedateerd en ondertekend verzoek** richten. |
| Dat mag u **ter plaatse** afgeven of **versturen** **per post of per fax,** samen met een **identiteitsbewijs** (fotokopie van uw identiteitskaart waarop u de onnodige gegevens kan doorstrepen). |

## DPO

* Verplicht aan te stellen wanneer:

|  |
| --- |
| De verwerking van gegevens wordt verricht door een **overheidsinstantie** of **overheidsorgaan** **behalve** bij **gerechten in de uitoefening van hun rechterlijke taken.** |
| Een verwerkingsverantwoordelijke[[29]](#footnote-29) hoofdzakelijk is belast met verwerkingen die **regelmatige en stelselmatige observatie op grote schaal van betrokkenen** vereisen. |
| De verwerkingsverantwoordelijke hoofdzakelijk is belast met grootschalige verwerking van **bijzondere categorieën van gegevens** zoals strafrechtelijke veroordelingen en strafbare feiten. |

* Nodige middelen die ter beschikking gesteld moeten worden van een DPO

|  |
| --- |
| **Actieve ondersteuning van de functie** van de functionaris door het hogere management |
| Voldoende **tijd** voor de functionaris om zijn taken te vervullen |
| Voldoende steun qua **financiële middelen, infrastructuur** en (indien nodig) **personeel** |
| **Officiële communicatie over de aanwijzing** van de functionaris naar alle medewerkers |
| De **vereiste toegang** tot andere diensten binnen de organisatie zodat de functionaris van die andere afdelingen de **essentiële steun, input en informatie** ontvangt |
| **Doorlopende training** |

* Taken van een DPO:

|  |
| --- |
| De **naleving en verordening controleren** van de andere **gegevensbeschermingsbepalingen** van de EU en de **interne regels** van de verwerkingsverantwoordelijke en de verwerker |
| Bijstaan van de verwerkingsverantwoordelijke of verwerker in de **gegevensbeschermingseffectbeoordeling**[[30]](#footnote-30) |
| Bijstaan van de verwerkingsverantwoordelijke of verwerker in de **opmaak** van het **register** van de **verwerkingsactiviteiten** |
| **Samenwerken** met de **toezichthoudende autoriteit** |
| **Fungeren als contactpersoon**, zowel voor **interne** medewerkers als **externe** betrokkenen |

* Waarborgen om ervoor te zorgen dat een DPO zijn werk kan doen:

|  |
| --- |
| De functionaris ontvangt **geen instructies** hoe hij/ zij zijn taken moet uitvoeren |
| De functionaris kan **niet ontslagen of gestraft** worden voor de uitvoering van zijn/ haar taken |
| Er mag **geen belangenvermenging** zijn tussen de functionaris-taken en de eventuele andere taken of functies van de functionaris |

## Gegevensbeschermingseffectbeoordeling (GEB)

*Een GEB is een procedure om te evalueren of een verwerking van persoonsgegevens risico’s inhoudt voor de rechten en vrijheden van de persoons wiens data wordt verwerkt en hoe men deze risico’s kan beheersen. De AVG verplicht een GEB/ DPIA[[31]](#footnote-31) in bepaalde omstandigheden.*

1. *Waarom?*

De verplichting om een GEB uit te voeren kwam van richtlijn 95/46/EG en stelde dat je bij iedere verwerking van persoonsgegevens dit moest melden aan de toezichthoudende autoriteit. Dit leidde echter tot administratieve en financiële lasten, zonder dat dit het beschermingsniveau voor persoonsgegevens verbeterde. Daardoor legt het systeem nu accent op de verplichting van de verwerkingsverantwoordelijke om een voorafgaande GEB uit te voeren voor verwerkingen die waarschijnlijk een hoog risico met zich meebrengen met als doel deze risico’s te verminderen.

1. *Wanneer?*

Het uitvoeren van een GEB is enkel verplicht wanneer de gegevensverwerking een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De AVG lijst nog een paar gevallen op waarbij het uitvoeren van een GEB verplicht is:

|  |
| --- |
| Wanneer men gebruikt maakt van **systematische en uitgebreide** **beoordeling** van **persoonlijke aspecten** van **natuurlijke personen** (waaronder profilering) waarop dan **besluiten** worden gebaseerd die een natuurlijk persoon **wezenlijk** **treffen**. |
| Wanneer men aan **grootschalige verwerking** van **bijzondere categorieën** van **persoonsgegevens**/ gegevens met betrekking tot **strafrechtelijke veroordeling**/ gegevens met betrekking tot **strafbare feiten** doet. |
| Wanneer men gebruik maakt van **stelselmatige** en **grootschalige monitoring** van **openbaar toegankelijke ruimten**. |

1. *Hoe?*

Een GEB moet minstens de volgende elementen bevatten:

|  |
| --- |
| Een **gedetailleerde en duidelijke beschrijving** van de **beoogde verwerkingen** en de **verwerkingsdoeleinden**. Het register van de verwerkingsactiviteiten kan hier richtgevend zijn. |
| Een **beoordeling** van de **noodzaak** en de **evenredigheid** van de **verwerkingen** in functie van de **doeleinden**. |
| Een **beoordeling** van de **risico’s** voor de **rechten** en **vrijheden** van **betrokken.** |
| De **beoogde maatregelen** om de **risico’s** aan te pakken. |

1. *Wie?*

De verplichting tot het uitvoeren van een GEB rust op de verwerkingsverantwoordelijke. Het is zijn plicht om ervoor te zorgen dat de juiste personen betrokken worden bij de GEB:

|  |
| --- |
| * De **functionaris** voor de **gegevensbescherming** en/ of **veiligheidsconsulent** * De **ontwikkelaars** van **nieuwe** **toepassingen** * Zij die **strategische** **beslissingen** nemen **inzake** **projectontwikkeling** * De **personeelsleden** (of hun vertegenwoordigers) die **gebruik** zullen **maken** van de **persoonsgegevens** bij hun taken |

**Hoofdstuk 7: Hacking**

# Wat mag je hacken?

## Wetgeving

De wet maakt onderscheid tussen twee types hackers:

|  |
| --- |
| **Interne hackers:**  Deze **overschrijden** de **bevoegdheden** op het **eigen computersysteem**. Zij zijn **strafbaar indien** ze **slechte bedoelingen** hebben. |
| **Externe hackers:**  Deze **overschrijden** de **bevoegdheden** op een **extern computersysteem**. Zij zijn **altijd strafbaar,** zelfs al is het netwerk niet beveiligd. |

Hacking is in België niet toegestaan, zelfs al ben je een white-hat hacker. Er is sprake van een mogelijke wetswijziging die het toestaat om dit verbod op te heffen.

## Hackers-platform

Hoe kan je dan leren hacken als je niet mag hacken in België? Je hebt twee opties om te leren hacken:

|  |
| --- |
| Je kan ervoor kiezen om een **eigen netwerk** op te zetten (waarvan jij dus de **eigenaar** bent). Op dit netwerk kan je dan hacken (inbraak op eigen goederen bestaat immers niet). |
| Je kan een netwerk gebruiken dat als **testplatform** gebruikt wordt. Een goed en nuttig voorbeeld van zo’n testplatform is ‘**hackthebox.eu’**. Het is wel belangrijk dat je je aan de **regels** van dit platform houdt. |

# SQL injection

## Wat?

Bij SQL injection gebruikt de hackers meestal een vrij toegankelijk tekstveld. Dit kan een contactformulier op een website zijn of beter nog, een login-formulier. Achter zo’n formulier zit meestal een database query. Die stuurt je naar wat je hebt ingegeven en neemt dus aan dat je je aan de regels houdt. Maar als je iets anders invoert zoals:

|  |
| --- |
| test@test.com OR 1=1 |

Dan geeft hij je alle gebruikers terug. Dit is omdat ‘1=1’ altijd TRUE is. Zo kan je dus alle inlognamen zien maar mogelijk ook de paswoorden. Van hieruit kan de hacker op zoek gaan naar een admin-account zodat hij alle rechten heeft.

## Welke SQL-producten

Er zijn verschillende SQL-uitvoeringen maar elke fabrikant past de basis van SQL toe waardoor de enige verschillen tussen de uitvoeringen kleine verschillen in syntax zijn. Daarom zijn alle uitvoeringen even vatbaar voor SQL-injectie.

## Welke kennis

De enige benodigde kennis die een hacker nodig heeft voor SQL-injectie is een kennis van SQL. Daarnaast is een kennis van netwerken handig, tezamen met inzicht in communicatie tussen websites en databases maar dit is niet strikt noodzakelijk.

## Countermeasures

Je kan je als websitebeheerder hiertegen verdedigen door ervoor te zorgen dat bepaalde ingevoerde SQL-opdrachten niet uitgevoerd kunnen worden. Dit doe je door bepaalde parameters of prepared statements in je query in te werken. Op deze manier ga je da ingevoerde tekst als string nemen en niet als SQL-opdracht waardoor hij ‘test@test.com OR 1=1’ niet zal vinden want er zijn geen gebruikers met deze naam.

1. Een firewall is hardware of software die checkt of er informatie naar binnen/ buiten mag door middel van het scannen van die informatie. (Een hardware firewall is heel duur maar is wel beter.) [↑](#footnote-ref-1)
2. IAM of Identity en Acces Management houdt de totaalheid van business processen in die de elektronische identiteit van werknemers checkt om er zo voor te zorgen dat iedereen aan zijn eigen info kan en niet meer dan dat. [↑](#footnote-ref-2)
3. Zie hoofdstuk 5. [↑](#footnote-ref-3)
4. Een andere naam voor een virus zou infector kunnen zijn omdat een virus eigen code toevoegt aan bestanden. [↑](#footnote-ref-4)
5. Deze vingerafdruk kan een algoritme ( het gedrag ervan) of een hash (een terugkerend cijferpatroon) zijn. [↑](#footnote-ref-5)
6. DDOS staat voor Distributed Denial of Service. Dit houdt in dat men heel veel geïnfecteerde computers tegelijk een pagina laat open waardoor deze pagina platligt. De aanval is dus bedoelde om een computer, computernetwerk of een dienst niet of moeilijker bereikbaar te maken voor mogelijke gebruikers. [↑](#footnote-ref-6)
7. Een kernel is de kern van het besturingssysteem. [↑](#footnote-ref-7)
8. Cracker staat voor Criminal hacking. Een cracker probeert dus ongeautoriseerde toegang tot een systeem te verkrijgen. [↑](#footnote-ref-8)
9. De term “hat” staat voor bediende. Dit is omdat een bediende iemand is die zijn handen niet vuilmaakt en daarom heeft hij de mogelijkheid om een hoed te dragen. [↑](#footnote-ref-9)
10. Een framework is een geheel van softwarecomponenten dat gebruikt kan worden bij het programmeren van applicaties. Ook de afspraken over hoe die componenten gebruikt worden binnen een groep ontwikkelaars en welke code-standaarden en bibliotheken gebruikt worden kunnen onderdeel zijn van een framework. [↑](#footnote-ref-10)
11. Een UPS is een Uninterruptible Power Supply/ Source. Dit is een elektrisch apparaatje dat zorgt voor elektriciteit in noodtoestanden. Het verschil tussen een UPS en een noodsysteem/ standby generator is dat een UPS bijna direct kan reageren op stroomonderbrekingen. Een UPS heeft slechts een beperkte energie maar dit is meestal voldoende om de generators/ het noodsysteem in werking te laten treden of om de apparaten correct af te zetten. [↑](#footnote-ref-11)
12. Een false positive komt voor wanneer je een positief resultaat krijgt (bijvoorbeeld: ‘Dit is een virus.’) terwijl het resultaat eigenlijk negatief moest zijn. [↑](#footnote-ref-12)
13. UTM staat voor Unified Threat Management. Dit kan je eigenlijk zien als een combinatie van verschillende veiligheidsmaatregelen. Een typisch UTM-pakket bevat vaak een netwerk firewall, intrusion detection, een antivirusprogramma, anti-spam software, antimalware, content filtering en nog veel meer. [↑](#footnote-ref-13)
14. Een passphrase is een zin die je gebruikt als wachtwoord. Deze zinnen moet echter niet grammaticaal correct zijn. [↑](#footnote-ref-14)
15. Een pakketgeschakeld netwerk duidt erop dat op een LAN of ander netwerk de over te zenden gegevens opgesplitst worden in kleinere pakketten met variabele grootte. [↑](#footnote-ref-15)
16. Een NIC is een **N**etwork **I**nterface **C**ard. [↑](#footnote-ref-16)
17. AES is de vervanger van DES (**D**ata **E**ncryption **S**tandard). [↑](#footnote-ref-17)
18. Een BSSID wordt gebruikt voor meerdere, overlappende WLANs met meerde APs. Het is het MAC-adres van het AP. [↑](#footnote-ref-18)
19. Een audit is het nakijken van een proces. Zo kan een auditor op een bedrijf de boekhouding nakijken. [↑](#footnote-ref-19)
20. Een control framework is een datastructuur die de interne controle van een bedrijf organiseert en categoriseert. De bedoeling van een control framework is het creëren van business value en het minimaliseren van risico. [↑](#footnote-ref-20)
21. Dit is een ISO-standaard voor informatiebeveiliging. Er staat in beschreven hoe informatiebeveiliging procesmatig ingericht zou kunnen worden. Als een bedrijf hiervan een certificaat haalt, betekent dit dat het bedrijf heel veilig probeert te werken. [↑](#footnote-ref-21)
22. Als een audit niet binnen de afgesproken tijd uitgevoerd wordt dan moet het audit-bedrijf een schadevergoeding betalen aan de klant. Echter, als de klant niet op tijd informatie stuurt, dan heeft het auditbedrijf ook recht op een schadevergoeding. [↑](#footnote-ref-22)
23. Deze dienen voor wanneer er dingen gebeuren die ervoor zorgen dat de auditor te laat is maar hij kan er niet aan doen (bvb: de stroom ligt plat en er zijn geen generatoren). [↑](#footnote-ref-23)
24. Een persoonsgegeven is iedere informatie betreffende een persoon die rechtstreeks of onrechtstreeks geïdentificeerd kan worden. Dit is een zeer breed begrip. Er wordt een onderscheid gemaakt tussen vertrouwelijke/ publiek toegankelijke en professionele/ niet professionele informatie. [↑](#footnote-ref-24)
25. Dit is echter wel beperkt: als de rechter/ overheid/ ziekenhuis zegt dat ze deze gegevens nog nodig hebben dan mag dit niet. Zo moet een ziekenhuis gegevens zeker 30 jaar bewaren. Ook als je iets betaalt en je wilt vergeten worden dan kan je pas na 10 jaar vergeten worden want dit is hoelang de factuur bijgehouden moet worden. [↑](#footnote-ref-25)
26. **D**ata **P**rotection **O**fficer: Deze persoon controleert of de GDPR wordt nageleefd. In sommige bedrijven is het verplicht om een DPO te hebben maar zelfs wanneer een bedrijf niet verplicht is er één te hebben dan kan dit aangeraden worden. [↑](#footnote-ref-26)
27. Dit houdt in dat men verplicht is om een register/ documentatie bij te houden van alle verwerkingen die binnen een organisatie uitgevoerd worden zodat men op elk moment verwerkingen van persoonsgegevens kan verantwoorden. [↑](#footnote-ref-27)
28. Als de rechter/ overheid/ ziekenhuis zegt dat ze deze gegevens nog nodig hebben dan mag dit niet. Zo moet een ziekenhuis gegevens zeker 30 jaar bewaren. Ook als je iets betaalt en je wilt vergeten worden dan kan je pas na 10 jaar vergeten worden want dit is hoelang de factuur bijgehouden moet worden. [↑](#footnote-ref-28)
29. Een verwerker is belast met een aantal kerntaken rond het verwerken van gegevens. Dit verschilt natuurlijk van bedrijf tot bedrijf. Zo kan een verwerker belast zijn met de gegevensverwerking door onderwijsinstellingen met betrekking tot hun leerlingen of studenten. [↑](#footnote-ref-29)
30. Een GEB of een gegevensbeschermingseffectbeoordeling wordt ook wel een DPIA (Data Protection Impact Assessment) genoemd. Dit houdt in dat er een risicoanalyse wordt gemaakt van de dataverwerking in een bedrijf voor de verwerking start zodat je maatregelen kunt nemen om die risico’s te verkleinen. [↑](#footnote-ref-30)
31. Dit is de Engelse term voor een GEB. [↑](#footnote-ref-31)