Cybersecurity 1: Samenvatting

Gilles De Praeter

Inhoudstabel

[1. Een wereld van experten en criminelen 3](#_Toc58323532)

[1.2 Criminelen vs specialisten 3](#_Toc58323533)

[1.3 Typische cyberaanvallen 4](#_Toc58323534)

[1.4 Verspreiding van cyberaanvallen 5](#_Toc58323535)

[1.5 Nood aan experten 6](#_Toc58323536)

[2. De cybersecurity kubus 7](#_Toc58323537)

[2.1 De 3 dimensies van de cybersecurity kubus 7](#_Toc58323538)

[2.2 De CIA-driehoek 7](#_Toc58323539)

[2.3 De 3 staten van data 8](#_Toc58323540)

[2.4 Beveiligingsmaatregelen 9](#_Toc58323541)

[2.5 Het cybersecurity ISO model 9](#_Toc58323542)

[3. Bedreigingen, aanvallen en kwetsbaarheden 10](#_Toc58323543)

[3.1 Malware en kwaadaardige code 10](#_Toc58323544)

[3.2 Misleiding en oplichting 12](#_Toc58323545)

[3.3 Cyber aanvallen 12](#_Toc58323546)

[4. De kunst van het beschermen van geheimen 14](#_Toc58323547)

[4.1 Cryptografie 14](#_Toc58323548)

[4.2 Toegangscontrole 17](#_Toc58323549)

[4.3 Data verduisteren 20](#_Toc58323550)

[5. Het verzekeren van integriteit 21](#_Toc58323551)

[5.1 Soorten integriteitscontroles 21](#_Toc58323552)

[5.2 Digitale handtekeningen 24](#_Toc58323553)

[5.3 Certificaten 25](#_Toc58323554)

[6. Het 5x9 principe 26](#_Toc58323555)

[6.1 Hoge beshcikbaarheid 26](#_Toc58323556)

[6.2 Maatregelen om de beschikbaarheid te verbeteren 27](#_Toc58323557)

[6.3 Incident response 29](#_Toc58323558)

[6.4 Disaster recovery 30](#_Toc58323559)

[6.5 verkenning en enumeratie 31](#_Toc58323560)

[6.5.1 Verkenningsfase: 31](#_Toc58323561)

[6.5.2 Scanningsfase: 33](#_Toc58323562)

[7. Het beschermen van een ICT omgeving 37](#_Toc58323563)

[7.1 Systemen en apparaten beschermen 37](#_Toc58323564)

[7.2 Server Hardening 39](#_Toc58323565)

[7.3 Netwerk Hardening 40](#_Toc58323566)

[7.4 Fysieke beveiliging 41](#_Toc58323567)

[8. Werken als een cybersecurity-specialist 42](#_Toc58323568)

[8.1 De verschillende cybersecurity domeinen 42](#_Toc58323569)

[8.2 De ethiek van werk in cybersecurity 43](#_Toc58323570)

[8.3 Cybersecurity profielen 45](#_Toc58323571)

[8.4 De volgende stap 45](#_Toc58323572)

# 1. Een wereld van experten en criminelen

## 1.2 Criminelen vs specialisten

Hackers:

* White hat hackers: goede hackers: zoeken zwakke punten om de beveiliging van systemen te verbeteren.
* Gray hat hackers: tussen de 2 andere types: vinden zwakke punten en melden dit als het samenvalt met hun agenda.
* Blackhat hackers: onethische criminelen die hacken voor persoonlijk gewin of andere kwaadaardige redenen.

Cybercriminelen:

* Script kiddies:
  + Tieners of hobbyisten
  + Grappen of vandalisme
  + Weinig of geen vaardigheid
  + Gebruiken vaak bestaande tools of instructies op het internet om aanvallen uit te voeren
* Vulnerability brokers (=kwetsbaarheidsbemiddelaars):
  + Gray hat hackers
  + Exploits ontdekken en deze aan leveranciers rapporteren, eventueel voor geldprijzen of beloningen
* Hacktivisten:
  + Gray hat hackers die zich verzamelen
  + Protesteren tegen politieke en sociale ideeën door atikelen en video’s te plaatsen, gevoelige informatie lekken en DDoS-aanvallen
* Cybercriminelen:
  + Black hat hackers
  + Zelfstandig of voor grote cybercrime-organisaties werken
* Door de staat gesponsorde hackers:
  + Ofwel white ofwel black hat hackers -> afhankelijk van perspectief persoon
  + Overheidsgeheimen stelen, inlichtingen verzamelen en netwerken saboteren
  + Doelwitten: buitenlandse regeringen, terroristische groeperingen en bedrijven
* Gecoördineerde acties tegen cybercriminelen:
  + Vulnerability databases:
    - Publiek beschikbare databases van gekende kwetsbaarheden
    - Vb in vs: de nation common vulnerabilities and exposures (CVE) -database
  + Early warning systems:
    - Systemen voor vroegtijdige waarschuwing
    - Vb: honeynet-project -> biedt een honeymap met real-time visualisatie van aanvallen
  + Share cyber intelligence:
    - Het delen van cyber intelligence, vaak door samenwerking tussen de publieke en private sector
    - Vb: infraguard -> samenwerkingsverband tussen de publieke en private sector met als doel het delen van info om aanvallen te voorkomen
  + ISM-normen:
    - Standaarden en normen voor informatiebeveiligingsbeheer die een kader vormen voor het implementeren van beveiligingsmaatregelen binnen een organisatie
    - **Vb: ISO 27000-normen!!!**

## 1.3 Typische cyberaanvallen

* Cyberbeveiligingsdreiging: is de mogelijkheid dat zich een schadelijke gebeurtenis, zoals een aanval, voordoet
* Cyberkwetsbaarheid: is een zwakte die een doelwit vatbaar maakt voor een aanval
* Interessante data van organisaties:
  + Persoonlijke informatie
  + Medische gegevens
  + Onderwijsgegevens
  + Werkgelegenheid gegevens
  + Financiële gegevens
* Doelwitten: netwerkdiensten zoals DNS, HTTP en online databases zijn de belangrijkste doelwitten voor cybercriminelen
* Criminelen gebruiken vaak:
  + Sniffing tools: bewaart en neemt alle verkeer over een netwerk op
  + Frauduleuze (rogue) apparaten: zoals valse wifi-toegangspunten
  + Valse berichten
* Hackers richten zich vaak ook tot netwerken van de industrie. Typische domeinen zijn:
  + Productie:
    - Branchecontroles
    - Automatisering
    - SCADA
  + Energieproductie en energiedistributie:
    - Elektrische distributie en smart grid
    - Olie en gas
  + Communicatie:
    - E-mail
    - Telefoon
    - Berichten
  + Transportsystemen:
    - Vliegreizen
    - Het spoor
    - Op de weg
* Beschermen op:
  + Persoonlijk vlak: iedereen moet zijn of haar identiteit, gegevens en computerapparatuur beschermen
  + Bedrijfsniveau: medewerkers moeten de reputatie, gegevens en klanten van de organisatie beschermen
  + Staatsniveau: moeten veiligheid burgers verzekeren -> vaak in tegenstrijd met de privacy

## 1.4 Verspreiding van cyberaanvallen

* Interne aanvallen:
  + Afkomstig van interne gebruiker
  + Grotere schade: rechtstreeks toegang tot het gebouw en de bijhorende infrastructuur/apparatuur
  + Kennis van het bedrijfsnetwerk, de bronnen en de vertrouwelijke gegevens
  + Eventueel ook kennis van beveiligingsmaatregelen, beleidsregels en hogere niveaus van beheerdersrechten
* Externe aanvallen:
  + Maken misbruik van kwetsbaarheden in netwerkapparaten, of doen aan social engineering om toegang te krijgen
* Bedreigingen door de opkomst van:
  + Mobiele apparaten: BYOD = bring your own device -> onvermogen om centraal te beheren en te bewerken
  + The internet of things (IoT): de verzameling technologieën die de verbinding van verschillende apparaten met het internet mogelijk maakt -> heeft invloed op de hoeveelheid gegevens en netwerken die moet worden beschermd
  + Big data: datasets die groot en complex zijn waardoor traditionele dataverwerkingstoepassingen ontoegankelijk zijn -> uitdagingen en kansen op 3 gebieden:
    - Het volume gegevens
    - De snelheid van de gegevens
    - De verscheidenheid of het bereik van gegevenstypen en bronnen
* Geavanceerde wapens:
  + Advanced persistent threat (APT): een voortdurende computerhack die onder de radar plaatsvindt tegen een specifiek object
  + Algoritme-aanvallen:
    - Kunnen zelfrapportagegegevens van het systeem volgen, zoals het energieverbruik van een computer, en die info gebruiken om doelen te selecteren of valse waarschuwingen te activeren
    - Zijn sluwer omdat ze gebruik maken van ontwerpen die worden gebruikt om energiebesparingen te verbeteren, systeemstoringen te verminderen en de efficiëntie te verbeteren
  + Intelligente selectie van slachtoffers: niet per se de zwakste schakel is het doelwit
* Federatief identiteitsbeheer:
  + Meerdere ondernemingen die hun gebruikers dezelfde identificatiegegevens laten gebruiken om toegang te krijgen tot de netwerken van alle ondernemingen in de groep
  + Doel: identiteitsinfo automatisch over kasteelgrenzen heen te delen
  + Beschermen door inlogmogelijkheid te koppelen aan een geautoriseerd apparaat
  + Vb: je kan je op verschillende sites inloggen met je facebook account bv, ook al heeft de website niks met fb te maken
* Telefonische denial of service (TDoS) -aanval: telefoongesprekken tegen een doeltelefoonnetwerk (bv de hulpdiensten) dat het systeem vasthoudt en verhindert dat legitieme oproepen binnenkomen
* VoIP-systemen = Voice-over-IP-systemen: bellen via IP-netwerken ipv de vaste lijn -> zoals skype: bellen via het internet (= een IP-systeem), ander vb: bedrijfsnetwerk

## 1.5 Nood aan experten

National Institute of Standards and Technologies (NIST) heeft een raamwerk gecreëerd voor bedrijven en organisaties die cyberbeveiligingsprofessionals nodig hebben. Het deelt cybersecuritywerk in 7 categorieën in:

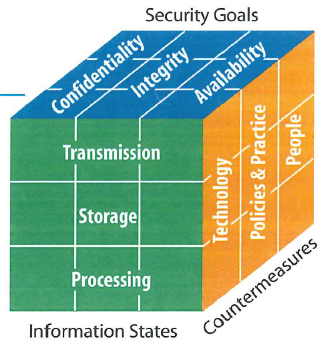
* Operate and maintain: het bieden van ondersteuning, het beheer en het onderhoud die nodig zijn om de prestaties en beveiliging van het IT-systeem te waarborgen
* Protect and defend: omvat de identificatie, analyse en beperking van bedreigingen door interne systemen en netwerken
* Investigate: het onderzoek naar cybergebeurtenissen en/ of cybercriminaliteit waarbij IT-middelen zijn betrokken
* Collect and operate: gespecialiseerde ontkennings- en misleidingsoperaties en het verzamelen van cyberbeveiligingsinformatie
* Analyze: zeer gespecialiseerde beoordeling en evaluatie van inkomende cyberbeveiligingsinformatie om te bepalen of deze nuttig is voor inlichtingen
* Oversight and development: voorziet in leiderschap, management en richting om de cyberveiligheid effectief uit te voeren
* Securely provision: het conceptualiseren, ontwerpen en bouwen van veilige IT-systemen

Certificeringen:

* CompTIA-Security +: een door CompTIA gesponsord testprogramma dat de competentie op het gebied van informatieborging certificeert
* EC-Council Certified Ethical Hacker (CEH): certificering op gemiddeld niveau dat cybersecurity-specialisten beschikken over vaardigheden en kennis voor verschillende hackpraktijken
* SANS GIAC-Security Essentials (GSEC): cybersecurity-specialisten begrijpen beveiligingsterminologie en -concepten en beschikken over de vaardigheden en expertise die nodig zijn voor ‘hands-on’ beveiligingsrollen
* (ISC)^2 Certified Information Systems Security Professional (CISSP): certificering voor cybersecurity-specialisten met veel technische en managementervaring
* ISACA Certified Information Security Manager (CISM): cybersecurity-specialisten verantwoordelijk voor het beheren, ontwikkelen en toezicht houden op informatiebeveiligingssytemen op bedrijfsniveau
* Cisco Certified Network Associate Security (CCNA Security): valideert dat een cybersecurity-specialist over de kennis en vaardigheden beschikt om Cisco-netwerken te beveiligen

# 2. De cybersecurity kubus

## 2.1 De 3 dimensies van de cybersecurity kubus

* Beveiligingsprincipes:
  + Identificeert het doel van beveiliging
  + Er zijn 3 principes (de CIA-driehoek):
    - Vertrouwelijkheid (confidentially)
    - Integriteit (integrity)
    - Beschikbaarheid (availability)
  + Helpen cybersecurity-specialisten om prioriteiten te stellen om de cyberwereld te beveiligen
* De staten van data (3):
  + Data in rust/ opslag
  + Data tijdens het verzenden
  + Data tijdens het verwerken
* Beveiligingsmaatregelen (3 types):
  + Technologieën: Toestellen en producten die gebruikt worden om informatie te beschermen en cybercriminelen af te weren
  + Beleid en praktijken: procedures en richtlijnen die de burgers van de cyberwereld veilig houden en aansporen om goede praktijken te volgen
  + Personen: Men is zich bewust van en kent de gevaren van de cyberwereld
* McCumber cube:

## 2.2 De CIA-driehoek

* Vertrouwelijkheid (confidentially):
  + Wie mag dit zien?
  + Verhindert bekendmaking van informatie aan onbevoegde personen, bronnen en processen
  + Organisaties moeten personeel opleiden om goed om te gaan met gevoelige info en zichzelf en hun organisatie te beschermen tegen aanvallen
  + Kan verkregen worden door:
    - Encryptie
    - Authenticatie
    - Toegangscontrole: omvat beschermingsmaatregelen die onbevoegde toegang tot computers, netwerken, databanken of andere databronnen verhindert. Deze maatregelen worden in 3 categorieën onderverdeeld:
      * Authenticatie (Authentication): Wie mag iets doen?
      * Autorisatie (Authorisation): Wat mag iemand wel/ niet doen?
      * Boekhouding (Accounting): wie heeft wat gedaan?
* Integriteit (integrity):
  + Klopt dit wel?
  + De nauwkeurigheid, consistentie en betrouwbaarheid van data zolang die data bestaat
  + Integriteit garanderen via hashing, data validatie checks, data consistentie checks en toegangscontroles
  + Integriteit is afhankelijk van de data: fb controleert posts niet, overschrijvingen moeten 100% juist zijn
  + Een integriteitscontrole is een manier om te bekijken of een verzameling van data nog steeds correct is. Hiervoor wordt vaak een hash functie gebruikt.
* Beschikbaarheid (availability):
  + Kan ik eraan wanneer ik het nodig heb?
  + Informatiesystemen moeten op elk moment beschikbaar zijn
  + Maatregelen om beschikbaar te blijven: redundantie (Meermalen voorkomen van dezelfde informatie), backups, verhoogde weerstand, onderhoud, up-to-date software en OS, noodplannen om terug online te komen na een onvoorziene omstandigheid, gebruik van nieuwe technologieën, detecteer ongebruikelijke activiteit en beschikbaarheidstesten
  + Altijd-online systemen (servers bv) hebben typisch 3 pijlers:
    - Vermijd zwakke punten (single point of failure)
    - Zorg voor betrouwbare overdrachtsystemen
    - Detecteer storingen zodra ze zich voordoen

## 2.3 De 3 staten van data

* Data in rust:
  + Data opgeslagen op opslagapparaten (harde schijven, usb, databanken, ..) dat niet wordt gebruikt door personen of processoren
  + Opslagapparaten kunnen lokaal (harde schijf, usb, ..) of gecentraliseerd op afstand (dropbox, google drive, ..) aangesloten zijn
  + Data kan zo verloren of gestolen worden: harde schijf kapot, laptop kwijt, ..
* Data tijdens het verzenden:
  + Verschillende manieren om data te verzenden:
    - Sneaker net: gebruikt opslagapparaten om data tussen computers over te zetten (usb’s, draagbare harde schijf, ..)
    - Bedraad netwerk: gebruikt koperkabels
    - Draadloos netwerk: gebruikt elektromagnetische straling (kan door iedereen in de buurt ‘gehoord’ worden
  + Enkele uitdagingen voor beveiliging:
    - Cybercriminelen kunnen data tijdens het verzenden afluisteren, kopiëren of stelen (vertrouwelijkheid)
    - Cybercriminelen kunnen data tijdens het verzenden aanpassen (integriteit)
    - Cybercriminelen kunnen data tijdens het verzenden verhinderen of verstoren (beschikbaarheid)
* Data tijdens de verwerking:
  + De data tijdens de invoer, aanpassingen, berekeningen of uitvoer
  + Verschillende methodes om data te verzamelen: manuele invoer, uploaden van bestanden, dataverzameling van sensoren, .. -> allemaal mogelijke bedreigingen voor de integriteit
  + Data kan aangepast worden door manuele veranderingen door gebruikers, programma’s die de data wijzigen, defecte apparaten, .. Enkele voorbeelden van data aanpassing: encoderen/ decoderen, compressie/ decompressie, encryptie/ decryptie
  + Corrupte data: data dat zodanig wordt aangepast dat het fouten bevat of onbruikbaar wordt

## 2.4 Beveiligingsmaatregelen

* Technologieën:
  + Software-gebaseerd: bv virusscanner of firewall op laptop
  + Hardware-gebaseerd: bv firewall apparaat op het netwerk
  + Netwerk-gebaseerd: bv verplicht aanmelden wanneer je met wifi verbindt
  + Cloud-gebaseerd: Beveiliging ligt bij cloud-provider bv dropbox, google drive -> is jouw data daar veilig? Wat als zij gehackt worden? Is ze dan nog van jou?
* Opleidingen en trainingen:
  + Geef opleidingen in bedrijven aan werknemers
  + Maak Cybersecurity een werkvereiste
  + Evaluatie op cybersecurity
* Beleid en procedures:
  + Er bestaan verschillende standaarden, richtlijnen en procedures om een cybersecuritybeleid uit te stippelen
  + Cybersecurity beleid: een reeks van doelstellingen voor een organisatie dat gedragsregels, systeemvereisten voor soft- en hardware, .. bepaalt voor gebruikers en administratoren -> bv: paswoord om de 6 maand veranderen, firewall apparaat, elk account beveiligd met 2FA,…

## 2.5 Het cybersecurity ISO model

* Het international organization for standardization (ISO) / international electrotechnical commission (IEC) hebben een volledig framework opgesteld om het beveiligen van data in goede banen te leiden. Dit framework noemt het ISO-model -> hulpmiddel om complexe problemen te begrijpen en aan te pakken
* Opgesteld in 2005 en gepubliceerd door het ISO
* Door velen gebruikt als het model voor cybersecurity
* Het ISO 27000 model is bruikbaar voor elk type organisatie en bevat controle doelstellingen in de vorm van een checklist

# 3. Bedreigingen, aanvallen en kwetsbaarheden

## 3.1 Malware en kwaadaardige code

Cybercriminelen vallen de toestellen van de gebruikers aan door het installeren van kwaadaardige code

Verschillende soorten malware:

* Virussen:
  + Een computervirus is een kwaadaardig stukje code die vasthangt aan een uitvoerbaar bestand.
  + Hebben een zekere vorm van actie nodig van de eindgebruiker. De virussen kunnen dan onmiddellijk of op een bepaald moment worden geactiveerd
* Worms:
  + Een stukje kwaadaardige code die zich kenmerkt doordat het zichzelf repliceert door gebruik te maken van een kwetsbaarheid in het netwerk.
  + Ze gaan ook vaak het netwerk vertragen.
  + Een virus heeft een host programma nodig om te draaien, een worm kan dit op zichzelf. Behalve de initiële infectie, heeft de worm geen interactie meer nodig van de gebruiker. De worm doet zelf al het werk
* Trojaanse paarden:
  + Malware die verborgen zit in gewenste bestanden zoals foto’s of een game zonder de gebruiker hiervan weet.
  + Verschilt van een virus omdat een Trojan horse een niet-uitvoerbaar bestand (zoals een foto) infecteert
  + Geen programma dat beschadigingen zelfstandig aanbrengt aan de geïnfecteerde computer, zoals een virus wel doet
  + Moet door de gebruiker worden gekopieerd en kopieert zich niet zelf naar andere computers, zoals een worm wel doet.
* Logic bomb:
  + Een kwaadaardig programma die wordt geactiveerd op een bepaald moment (=trigger)

-> het wacht dus op de trigger om te activeren en schade toe te brengen

-> de trigger kan een bepaalde datum zijn, een ander programma dat wordt opgestart, een bepaalde actie die werd gedaan, …

* Ransomware:
  + Een computersysteem of data wordt geblokkeerd of geëncrypteerd tot het slachtoffer een geldsom betaalt.
  + De key om de data te decrypteren blijft dus geheim tot er betaald is, en wordt zelf dan soms niet gegeven.
* Backdoors en rootkits:
  + Een rootkit zal het operating system aanpassen en zo een backdoor creëren
  + Deze backdoor wordt dan gebruikt om het systeem binnen te dringen, zonder enige vorm van authenticatie

E-mail en browser aanvallen:

* Spam:
  + Meestal advertenties, maar soms verwijzingen naar kwaadaardige links met mogelijks misleidende informatie
* Spyware:
  + Probeert informatie te vergaren over de gebruiker en deze door te sturen naar een externe partij
  + Vaak worden de beveiligingsinstellingen aangepast
  + Kan gaan over keystrokes verzamelen of data capture
  + Doel: geld verdienen (meestal)
* Adware:
  + Typisch zijn de lastige pop-ups die proberen op één of andere manier winst op te leveren voor de auteur.
  + Advertentie-ondersteunende software
  + Behoort gemakshalve tot de spywarecategorie
* Scareware:
  + Probeert de gebruiker te overtuigen door ze bang te maken
  + Bv: een dialoogvenster van het besturingssysteem -> error…
* Phishing:
  + Aasaanval
  + Password Harvesting Fishing
  + Vorm van fraude
  + Aanvaller probeert informatie (logingegevens, credit card, ..) te verkrijgen van het slachtoffer
  + Vaak krijg je via social media een link naar een fake loginscherm (bv van de bank) waar je, bij het inloggen, je gegevens bloot legt aan de aanvaller.
* Spear phishing:
  + Minder algemeen dan phishing, maar wel beiden via e-mail
  + Specifiek gericht op een individu, organisatie of bedrijf
* Cat phishing:
  + Vaak wordt een valse identiteit gemaakt om op die manier het vertrouwen van het slachtoffer te winnen
  + Bv: een liefdesrelatie op datingsite
* Vising:
  + Ofwel voice phishing
  + Vorm van criminele telefoonfraude, waarbij men social engineering gebruikt om toegang te krijgen tot persoonlijke en financiële info, met het oog op een financiële beloning
* Pharming:
  + Een samentrekking van ‘phising’ en ‘farming’
  + Grote aantallen internetgebruikers worden naar de nepwebsite van de hacker geleid.
  + Bestaande webpagina wordt overgenomen (kopie) door de fraudeur. De originele DNS- verwijzing wordt dus gewijzigd
* Whaling:
  + Een phishing aanval die als doelwit een hooggeplaatst persoon heeft
* Plugins:
  + Is een aanvulling op een computerprogramma -> hackers kunnen deze misbruiken
  + Plugins zoals Flash en Shockwave (Adobe) worden gebruikt om (browser) content te tonen die met hun software wordt gemaakt
* SEO poisoning:
  + Zoekmachines zoals Google tonen de resultaten op basis van de query van de gebruiker. Deze zoekresultaten worden geordend door middel van Search Engine Optimalization (SEO). Dit is een verzameling van technieken die er moet voor zorgen dat jouw website hoog scoort
  + Cyber criminelen misbruiken SEO om hun kwaadaardige software hoog in google laten te ranken
* Browser Hijacker:
  + Zorgt dat de browser instellingen worden gewijzigd. Zo kunnen criminelen zorgen dat jouw browser doorlinkt naar de website van de ‘klant’ van deze crimineel

## 3.2 Misleiding en oplichting

De kunst van het oplichten:

* Social engineering: het vertrouwen van je slachtoffer winnen om nadien van het slachtoffer iets te verlangen. Bv je kan je voordoen als iemand van de beveiligingsfirma en vragen om de poort te openen
* Pretexting: het slachtoffer wordt opgebeld en gevraagd om gevoelige informatie vrij te geven om identificatie mogelijk te maken. Er wordt bv een creditcardnummer gevraagd aan het slachtoffer
* Something for something: wanneer een attacker persoonlijke informatie over iemand vraag en in ruil iets in de plaats geeft zoals een cadeau

Soorten oplichting:

* Shoulder surfing en dumpster diving: het aflezen/meelezen van PIN-codes of wachtwoorden en dergelijke door gebruik van een camera, verrekijker, dichtbij te staan, …
* Impersonation en hoaxes: doen alsof je iemand anders bent, een hoax is een nepbericht zoals een valse email van het WWF
* Piggybacking en tailgating: het mee glippen met personen die wel toegang hebben tot een plaats met beperkte toegang
* Online, e-mail en web-based trickery: het bewust forwarden van hoax e-mails, grappige filmpjes en dergerlijke. Kan ingaan tegen bedrijfspolicy en kan bedrijven veel geld kosten

## 3.3 Cyber aanvallen

Soorten cyber aanvallen:

* Denial-of-Service (DoS) Attacks:
  + Een manier om een netwerk aan te vallen.
  + Resulteert in het niet beschikbaar zijn van een bepaalde netwerkservice
  + Groot risico -> veel tijd en geld verlies
  + Makkelijk uit te voeren
* Sniffing:
  + Alle netwerkverkeer die passeert aan NIC (Network Interface Card) bekijken
  + Speciale soft- en /of hardware
* Spoofing:
  + De werkelijkheid gaan vervalsen
  + De dader gaat kenmerken gaan aanpassen om te doen alsof hij iemand anders is.
  + Bv: bij email spoofing zal men de header (van..) aanpassen. Zo kan men doen alsof de email door iemand anders werd verstuurd,
  + Ook URL spoofing of IP spoofing
* Man-in-the-middle:
  + De cyber crimineel zal proberen informatie te stelen dat wordt verstuurd over een netwerk tussen twee toestellen. Hij kan ook de boodschap aanpassen en dus valse informatie te verspreiden tussen de hosts. De hosts zijn zich hiervan niet bewust.
  + Controle overnemen zonder de andere partijen dit weten
* Zero-day attacks:
  + Er wordt geprobeerd gebruik te maken van een kwetsbaarheid in software die nog niet gekend is.
  + Day zero verwijst naar het moment waar het lek ontdekt wordt.
* Keyboard logging:
  + Een computerprogramma die de toetsenbordaanslagen (keystrokes) gaat opnemen of loggen.
  + De software wordt op het toestel van het slachtoffer geïnstalleerd
  + Dader programmeert de software om na afloop de logfile of opname via e-mail door te sturen naar dader
  + Logfile kan dan gevoelige info bevatten zoals passwoorden, …

Draadloze en mobiele aanvallen:

* Grayware:
  + Apps die zich enerverend of ongewenst gaan gedragen, maar zijn geen grote gevaren zoals virus of trojan horse.
* SMiShing:
  + SMS Phising
  + Fake SMS (Short Message Service) gebruiken om valse berichten te sturen. Zo probeert de dader het slachtoffer te lokken naar een website (kan voor malware zorgen) of verleiden om te bellen naar een bepaald telefoonnummer (gevoelige info proberen verkrijgen).
* Frauduleuze (Rogue) Acces Point:
  + Wordt in het netwerk geplaatst en doet zich voor al een vertrouwelijk apparaat. Het zorgt ervoor dat mensen hun verkeer via dit Acces point versturen en zo kan het de data zien en analyseren
  + Laat toe om MitM-attacks uit te voeren

Applicatie aanvallen:

* Cross-site scripting (XSS):
  + Een kwetsbaarheid die wordt gevonden in webapplicaties. Zo kan je scripts injecteren.
  + Vaalt slachtoffer niet rechtstreeks aan, wel de website
  + Dader slaagt er soms in files te bekijken op de webserver die niet voor hem zijn bedoelt
* Code injections aanvallen:
  + Doelwit: databank die data voor website bevat
  + Via een SQL injection bv kan men proberen een SQL-databank aan te vallen
  + Men injecteert dan een query om deze uit te voeren
* Buffer overflow:
  + Wanneer data over zijn limiet gaat
  + Buffers: geheugen die door een applicatie wordt gebruikt
  + Door de data aan te passen en te vergroten zodat het de buffers overschrijdt, gebruikt de applicatie geheugen dat door een ander proces wordt gebruikt en krijg je een error -> applicatie crash of verlies van data
* Remote code executions:
  + De dader maakt gebruik van een kwetsbaarheid waarbij hij code vanop afstand kan uitvoeren
  + Over bv netwerk of internet kan je dan slachtoffer aanvallen
* ActiveX controls:
  + Stukjes software die worden geïnstalleerd als plug-in in een browser. Deze software kan dan bv de gewoontes van een gebruiker analyseren of het lezen van toetsaanslagen, …
* Java:
  + Wordt uitgevoerd via een interpreter (= vertaler), de Java Virtual Machine (JVM)
  + Normaal draait kwaadaardige code in de sandbox omgeving van de JVM, maar soms lukt het daders om deze sandbox te omzeilen en zo toch de code uit te voeren op het besturingssysteem van het slachtoffer
  + Dader maakt hierbij gebruik van een al dan niet bekende kwetsbaarheid in Java

Beschermen tegen deze aanvallen:

* First-line defense: programmeurs moeten stabiele code schrijven
* Alle user input van buitenaf beschouwen als vijandige of kwaadaardige code
* Alle user input valideren en controleren
* Alle software waaronder plug-ins up-to-date houden door updates regelmatig uit te voeren
* Niet alle updates worden automatisch uitgevoerd -> controleer zelf ook op updates
* Never ending story: nog veel meer beschermingsmaatregelen die we nog gaan leren

# 4. De kunst van het beschermen van geheimen

## 4.1 Cryptografie

* Cryptologie: de wetenschap van het maken en breken van geheime codes.
* Cryptografie:
  + Een manier om gegevens op te slaan en te verzenden, zodat alleen de beoogde ontvanger deze kan lezen of verwerken
  + Veel ouder dan computers (1000’en jaren) -> belangrijk middel voor uitwisselen van berichten in diplomatieke kringen
  + Moderne cryptografie: gebruik van algoritmen om gevoelige data te beschermen
* Berichten encrypteren/ decrypteren:
  + Specifiek algoritme, een cijfer/ cipher genaamd -> een reeks goed gedefinieerde stappen om berichten te versleutelen en ontsleutelen
  + Verschillende technieken om cijfertekst te maken:
    - Transpositie (omzetting) -> vb: transponeren matrix
    - Substitutie (vervanging) -> vb: karakters vervangen door andere
    - Eenmalig pad -> vb: een random sleutel (=pad) wordt opgeteld bij de plaintext en vervolgens wordt het resultaat omgezet naar een getal van 2 cijfers

Twee types algoritmen:

* Symmetrische algoritmen:
  + Zelfde sleutels voor encrypteren en decrypteren
  + Verzender en afzender kennen de sleutel voor communicatie begint
* Asymmetrische algoritmen:
  + Sleutelpaar = verschillende sleutels voor encrypteren en decrypteren
  + 1 sleutel is publiek (openbaar), andere is privé:
    - Vaak gebruikte term: publieke-sleutelcryptografie
    - Iedereen kan bericht encrypteren met publieke sleutel, enkel ontvanger kan decrypteren met private sleutel -> omgekeerd kan ook
  + Complexer en dus trager dan symmetrische algoritmen

Private-key versleuteling:

* Symmetrisch versleutelingsproces: vooraf gedeelde sleutel om gegevens te encrypteren en decrypteren (private-key versleuteling)
* Enkele van de algemene coderingsstandaarden voor de symmetrische codering:
  + DES -> Digital Encryption Standard:
    - Eenvoudig, encrypteert 64-bits blokken met 56-bits sleutel
    - Niet veilig -> niet bruikbaar
  + 3DES -> Triple DES:
    - 3x DES met andere sleutel voor minstens 1 van de drie passages
    - Sleutelsterkte: in praktijk 112-168 bits afhankelijk van gekozen combinatie
  + IDEA -> International Data Encryption Algorithm:
    - 64-bits blokken met 128-bits sleutel -> 8 transformatieronden op elk van de 16 blokken, die het resultaat zijn van het verdelen van de 64-bits blok
    - Vervanging van DES, gebruikt bij PGP (Pretty Good Privacy)
  + AES -> Advanced Encryption Standard:
    - 128-bits blokken, sleutel van 128, 192 of 256 bits
    - Goedgekeurd door NIST (National Institute of Standards and Technology)
    - Gebruikt door Amerikaanse overheid voor geheime informatie

Public-key versleuteling:

* Asymmetrisch versleutelingsproces: Verschillende sleutels voor encrypteren en decrypteren (public-key encryption)
  + Niet mogelijk om via 1 key de andere te achterhalen
* Enkele asymmetrische algoritmen:
  + RSA -> Rivest Shamir Adleman:
    - Gebruikt product van 2 heel grote priemgetallen met een gelijke lengte tussen de 100 en 200 cijfers
    - Vaak gebruikt in browsers om veilige verbinding te maken
  + Diffie-Hellman:
    - Biedt een elektronische uitwisselingsmethode om de geheime sleutel te delen
    - Vaak gebruikt door: SSL (Secure Sockets Layer), TLS (Transport Layer Security), SSH (Secure Shell), IPSec (Internet Protocol Security)
  + ElGamal:
    - Gebruikt Amerikaanse overheidsstandaard voor digitale handtekeningen
    - Gratis, niemand heeft patent
  + ECC -> Elliptic Curve Crypthography:
    - Alternatief voor RSA: Nulpunten van elliptische curven ipv. Priemgetallen
    - Gebruikt in VS door NSA voor het genereren van digitale handtekeningen en het uitwisselen van sleutels

Symmetrisch vs asymmetrische codering:

|  |  |
| --- | --- |
| Symmetrisch | Asymmetrisch |
| Snel | Niet nodig om beide sleutels te delen |
| Verbruikt weinig resources | Kan gebruikt worden voor encryptie en validatie (=handtekening) |
| Kan gebruikt worden voor korte en lange berichten | Gebruikt veel resources |
| Sleutel moet op veilige manier gedeeld worden | Enkel bruikbaar voor relatief kleine berichten |

* Symmetrische versleutelingssystemen zijn efficiënter en kunnen meer gegevens verwerken. Sleutelbeheer met symmetrische versleutelingssystemen is echter problematischer en moeilijker te beheren.
* Asymmetrische cryptografie is efficiënter in het beschermen van de vertrouwelijkheid van kleine hoeveelheden gegevens, en de grootte en snelheid ervan maken het veiliger voor taken zoals elektronische sleuteluitwisseling, wat een kleine hoeveelheid gegevens is in plaats van grote blokken gegevens te versleutelen.

Toepassingen:

* Eenmalig wachtwoord genererend token = hardware apparaat om een eenmalig wachtwoord te genereren (cfr. online banking). Een eenmalig wachtwoord is een automatisch gegenereerde numerieke of alfanumerieke reeks tekens die een gebruiker verifieert voor slechts één transactie van één sessie. Het nummer verandert elke 30 seconden of zo. Het sessiewachtwoord verschijnt op een display en de gebruiker voert het wachtwoord in.
* Elektronische betalingssector gebruikt 3DES
* Oudere besturingssystemen: DES om gebruikersbestanden en systeem gegevens te beschermen met wachtwoorden (niet meer veilig in 2020!)
* De meeste versleutelde bestandssystemen, zoals NTFS, gebruiken AES

Protocollen die asymmetrische sleutelalgoritmen gebruiken:

* Internet Key Exchange (IKE), een fundamenteel onderdeel van IPsec Virtual Private Networks (VPN’s).
* Secure Socket Layer (SSL), een manier om cryptografie in een webbrowser te implementeren (HTTPS maakt gebruik van SSL)
* Secure Shell (SSH), een protocol dat een veilige verbinding voor externe toegang tot netwerkapparaten biedt (remote inloggen op Linux toestel)
* Pretty Good Privacy (PGP), een computerprogramma dat cryptografische privacy en authenticatie biedt om de beveiliging van e-mailcommunicatie te vergroten
  + GPG = GNOME (Linux) implementatie van PGP –
  + Je kan GPG-sleutel toevoegen in GitHub om commits en tags digitaal te ondertekenen!

Voorbeeld:

* VPN = privénetwerk over het internet, veilig communicatiekanaal tussen 2 eindpunten (bv. 2 kantoren op verschillende geografische locatie)
  + VPN's gebruiken IPsec. IPsec is een reeks protocollen die zijn ontwikkeld om beveiligde services via netwerken te realiseren
  + IPsec-services maken authenticatie, integriteit, toegangscontrole en vertrouwelijkheid mogelijk
  + Met IPsec kunnen externe sites gecodeerde (encryptie) en geverifieerde (authenticatie) informatie uitwisselen.
  + Bescherming van data in beweging
  + Data in gebruik heeft geen enkele bescherming omdat de gebruiker de gegevens moet openen en wijzigen. Systeemgeheugen bevat die in gebruik zijn en kan gevoelige gegevens bevatten, zoals de coderingssleutel -> criminelen mogelijks toegang

## 4.2 Toegangscontrole

Soorten toegangscontrole:

* Fysieke toegangscontrole:
  + Daadwerkelijke barrières die worden ingezet om direct contact met systemen te voorkomen
  + Doel: Voorkomen onbevoegde toegang tot faciliteiten, apparatuur en andere bedrijfsmiddelen
  + Fysieke toegangscontrole bepaalt wie kan binnenkomen (of verlaten), waar ze kunnen binnenkomen (of verlaten) en wanneer ze kunnen binnenkomen (of verlaten).
* Logische toegangscontrole:
  + Omvat hardware- en softwareoplossingen die worden gebruikt om de toegang tot bronnen en systemen te beheren.
  + Omvat tools en protocollen voor identificatie, authenticatie, autorisatie en verantwoording (accountability)
* Administratieve toegangscontrole:
  + Beleid en procedures in organisaties
  + Controleren van ongeautoriseerde toegang
  + Gericht op personeel en zakelijke praktijken

Onderwerp vs object:

* Onderwerp:
  + Kan gebruiker of proces zijn
  + Wil iets doen met een object
* Object:
  + Kan bestand, poort of In- of uitvoerapparaat zijn
  + Onderwerp wil een object aanspreken

Toegangscontrole: dwingt af of een onderwerp de nodige toegang heeft tot het object, en een bepaalde actie kan/mag uitvoeren

Strategieën voor toegangscontrole:

* Verplichte toegangscontrole:
  + EN: Mandatory Access Control -> MAC
  + Beperkt de acties die een onderwerp op een object kan uitvoeren.
  + Een autorisatieregel dwingt af of een onderwerp al dan niet toegang heeft tot het object.
* Discretionaire toegangscontrole:
  + EN: Discretionary Access Control -> DAC
  + Verleent of beperkt objecttoegang bepaald door de eigenaar van het object.
  + Eigenaar kan rechten doorgeven aan een ander onderwerp
* Rolgebaseerde toegangscontrole:
  + EN: Role-based Access Control -> RBAC
  + Gebaseerd op de rol (= functie binnen een organisatie) van het onderwerp
  + Voor specifieke rollen zijn machtigingen vereist om bepaalde bewerkingen uit te voeren
  + Gebruikers verwerven machtigingen via hun rol
  + RBAC kan werken in combinatie met DAC of MAC door het beleid van beide af te dwingen
* Op regels gebaseerde toegangscontrole:
  + EN: Rule-based Access Control
  + Toegangscontrolelijsten (EN: Access Control Lists - ACL's) om toegang te verlenen
  + Een reeks regels is opgenomen in de ACL. De beslissing om al dan niet toegang te verlenen hangt af van deze regels.
  + Voorbeeld regel: geen enkele werknemer mag buiten kantooruren toegang hebben tot het salarisdossier

Identificatie: dwingt de regels af die zijn opgesteld door het autorisatiebeleid:

* Een onderwerp vraagt toegang tot een systeembron (= object)
* De toegangscontroles bepalen of toegang moet worden verleend of geweigerd
* Cybersecurity policies bepalen welke identificatiecontroles moeten worden gebruikt
* De gevoeligheid van informatie en informatiesystemen bepalen hoe streng de controles zijn
* De toename van datalekken heeft veel organisaties gedwongen hun identificatiecontroles te versterken

Authenticatiemethoden:

* What you know:
  + Iets dat de gebruiker weet
  + Wachtwoorden, pincodes, …
* What you have:
  + Iets dat de gebruiker in zijn bezit heeft
  + Smartcards, beveiligingssleutelhangers
* Who you are:
  + Een uniek fysiek kenmerk, zoals een vingerafdruk, netvlies of stem, die een specifieke gebruiker identificeert, wordt biometrie genoemd.
* Bij multi-factor authenticatie worden ten minste 2 verschillende authenticatiemethoden gebruikt.

Autorisatie: bepaalt wat een gebruiker kan doen na authenticatie:

* Toegang tot welke (netwerk) bronnen? Wat kan de gebruiker doen met de bronnen?
* Maakt gebruik van een set attributen die de toegang van de gebruiker tot het netwerk beschrijven.
* Het systeem vergelijkt deze attributen met de informatie in de authenticatiedatabase, bepaalt een reeks beperkingen voor die gebruiker en bezorgt deze aan de lokale router waarop de gebruiker is aangesloten.
* Een autorisatiebeleid legt de autorisatieregels vast voor beheren toegang

Verantwoording (accountability): herleidt een actie terug naar een persoon of proces dat de wijziging in een systeem aanbrengt, verzamelt deze informatie en rapporteert de gebruiksgegevens:

* Organisatie kan dit gebruiken voor audits of facturering
* Verzamelde gegevens kunnen zijn:
  + Inlogtijd gebruiker
  + Succesvol aangemeld?
  + Tot welke bronnen toegang?
* Hierdoor kan een organisatie acties, fouten en vergissingen tijdens een audit of onderzoek traceren.
* Implementatie van verantwoording via technologieën, beleid, procedures en opleidingen
* Logbestanden: gedetailleerde informatie op basis van gekozen parameters

Soorten beveiligingsmaatregelen:

* Preventieve maatregelen: voorkomen dat er iets gebeurt:
  + Preventieve toegangscontrole voorkomt dat ongewenste of ongeautoriseerde activiteiten plaatsvinden.
* Afschrikmiddel tegenover beloning:
  + Beloning moedigt mensen aan om het goede te doen
  + Afschrikmiddel weerhoudt hen ervan het verkeerde te doen
  + Enkel afschrikmiddelen vaak niet voldoende
* Detectieve maatregelen: om iets te ontdekken:
  + Bij toegangscontrole: ontdekken ongeautoriseerde activiteiten
  + Eenvoudige detectiesystemen: bv. bewegingsmelder of bewaker
  + Complexere detectiesystemen: bv. Inbraakdetectiesysteem
* Corrigerende maatregelen: gaan iets tegen dat ongewenst is:
  + Invoeren toegangscontroles nadat een systeem een bedreiging heeft ondervonden.
  + Corrigerende controles brengen het systeem terug naar een staat van vertrouwelijkheid, integriteit en beschikbaarheid.
  + Ze kunnen ook systemen herstellen naar een normale toestand nadat er ongeautoriseerde activiteiten hebben plaatsgevonden
* Herstelmaatregelen: zorgen voor terugkeer naar een normale toestand:
  + Toegangscontroles voor herstel herstellen bronnen, functies en mogelijkheden na een schending van een beveiligingsbeleid.
  + Herstelcontroles kunnen schade herstellen, naast het stoppen van verdere schade.
  + Deze controles hebben meer geavanceerde mogelijkheden dan corrigerende maatregelen
* Compensatieve maatregelen: proberen iets goed te maken:
  + Bieden opties voor andere controles om de handhaving ter ondersteuning van een beveiligingsbeleid te versterken
  + Compenserende controle kan substitutie zijn voor andere controle die niet mogelijk is

## 4.3 Data verduisteren

Gegevensmaskering:

* Gegevens beveiligen door door gevoelige informatie te vervangen door een niet-gevoelige versie.
* Niet-gevoelige versie ziet eruit en gedraagt zich als het origineel
  + Geen wijzigingen nodig aan applicaties of dataopslagfaciliteiten
* Meestal beperkt maskering de verspreiding van gevoelige gegevens binnen IT-systemen door vervangende gegevenssets te distribueren voor testen en analyse.
* Verschillende technieken om gegevens te wijzigen maar zinvol te houden:
  + Vervanging: vervangt gegevens door authentiek ogende waarden (garanderen anonimiteit)
  + Shuffling: leidt een vervangingsset af uit de gegevens die een gebruiker wil maskeren
    - Shuffling werkt goed voor bijvoorbeeld financiële data in een testdatabase

Steganografie:

* Verbergt gegevens in een ander bestand:
  + Bv grafisch, audio- of ander tekstbestand
* Geheime boodschap valt niet op:
  + Niemand zou ooit weten dat een foto daadwerkelijk een geheime boodschap bevatte door het bestand elektronisch of op papier te bekijken
* Er zijn verschillende componenten betrokken bij het verbergen van gegevens:
  + Ingebedde gegevens = geheim bericht
  + Omslagtekst verbergt gegevens die de stego-tekst produceren
    - Omslag en/of verborgen gegevens kunnen ook afbeelding of audio zij
  + Stego-key regelt het verbergingsproces

Gegevensverduistering (obfuscation):

* Het toepassen van gegevensmarkering en steganografietechnieken
* Verduistering: maakt de boodschap verwarrend, dubbelzinnig of moeilijker te begrijpen
* Een systeem kan opzettelijk berichten door elkaar halen om ongeautoriseerde toegang tot gevoelige informatie te voorkomen
* Softwarewatermerken:
  + Beschermen software tegen onbevoegde toegang of wijziging
  + Voegen een geheim bericht in het programma toe als bewijs van eigendom
  + Het geheime bericht is het softwarewatermerk Als iemand het watermerk probeert te verwijderen, is het resultaat een niet-functionele code

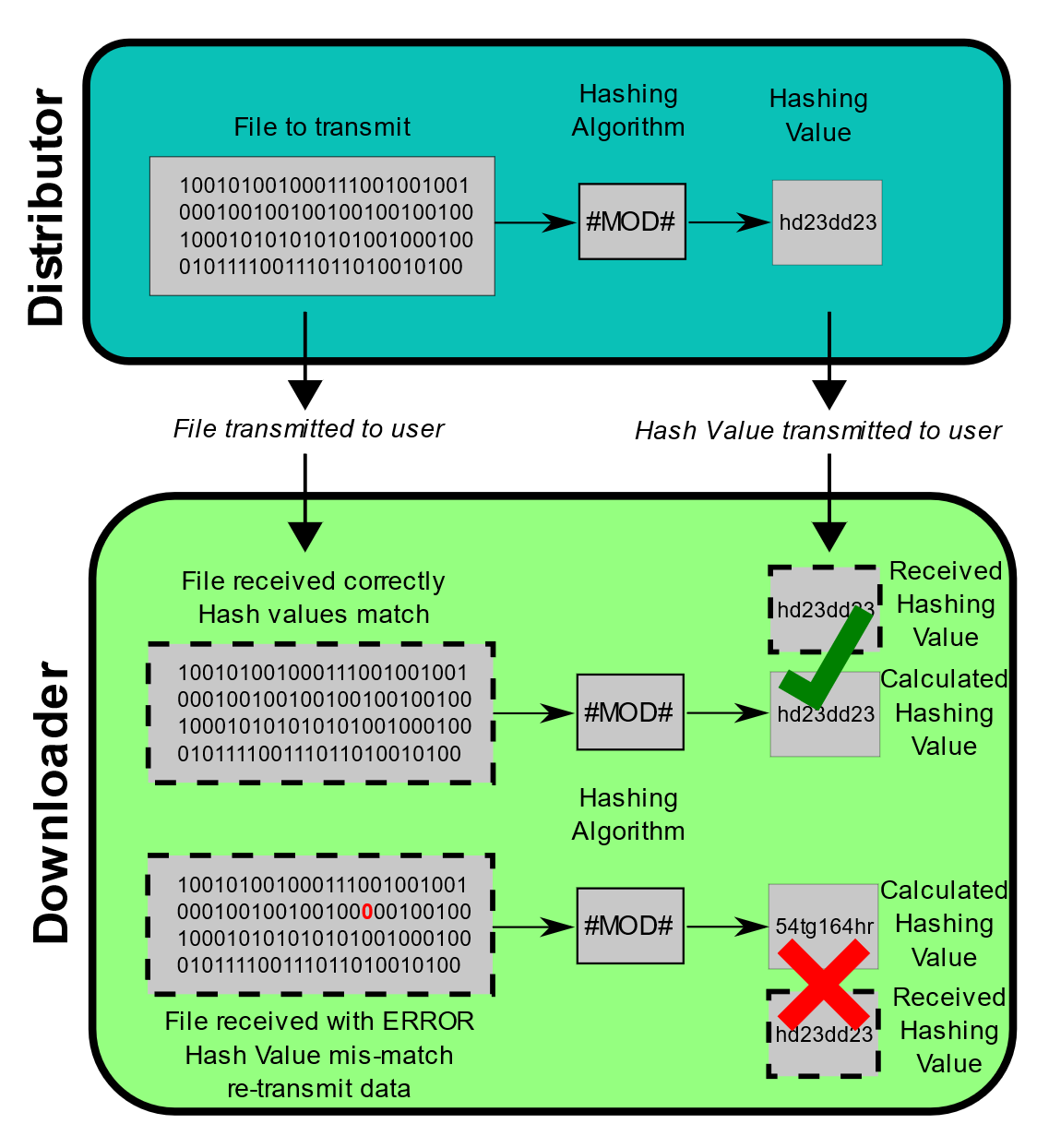
# 5. Het verzekeren van integriteit

## 5.1 Soorten integriteitscontroles

Hashing algoritmes:

* Vormt een reeks van bits om naar een reeks van een vast aantal bits
* Het is een wiskundige eenrichtingsfunctie.
  + Het is in de ene richting makkelijk te berekenen, maar onmogelijk te berekenen in de andere richting
* Een cryptografische functie heeft de volgende eigenschappen:
  + De input kan uit om het even welk aantal bits bestaan
  + De output heeft steeds hetzelfde aantal bits, ongeacht het aantal bits van de input
  + De hashfunctie is een eenrichtingsfunctie en is onmogelijk om te keren
  + Twee verschillende inputwaarden zullen steeds een verschillende outputwaarde geven
* 2 populaire hashing algoritmes:
  + Message Digest 5 Algorithm (MD5) ontwikkeld door Ron Rivest. Het geeft een 128-bits output terug
  + Secure Hash Algorithm ontwikkeld door het US National Institute of Standards and Technology (NIST). Hiervan bestaan verschillende varianten afhankelijk van het gewenst aantal bits van de output:
    - SHA-224 (224 bits)
    - SHA-256 (256 bits)
    - SHA-384 (384 bits)
    - SHA-512 (512 bits)

Toepassingen:

* Controleren op fouten in data
* Het veilig bewaren en controleren van paswoorden in databanken
* Identificeren van data aan de hand van een kleinere waarde (fingerprint)
* Gebruikt bij efficiënte opslag van data in hashtabellen

Veilig bewaren van paswoorden:

* Gebruikersnaam en paswoord worden vaak opgeslagen in databanken
* Databanken zijn een gewild doelwit van cybercriminelen. Een gelekte hoeveelheid gegevens uit een databank noemt een Data Breach (datalek)
* Velen hergebruiken dezelfde username (vaak hun e-mailadres) en paswoord. Als deze combinatie wordt gevonden in een data breach, wordt deze door cybercriminelen getest op andere websites. Dit is een grote oorzaak van hacks
* Het gebruik van 1 paswoord dat je telkens lichtjes aanpast per website heeft geen zin. De software van cybercriminelen houdt hier rekening mee
* Gebruik een paswoordmanager en gebruik een uniek paswoord per website!
* Poging 1: we slaan de gebruikersnaam en paswoord gewoon op in de databank. Bij het inloggen moeten we gewoon het volgende controleren:
  + Naam == naam in databank?
  + Paswoord == paswoord in databank?
  + Wordt ook “plaintext” opslag genoemd
  + Eenvoudig
  + Als iemand in de databank geraakt, kan hij meteen alle paswoorden uitlezen → GEVAARLIJK!
* Poging 2: we slaan de gebruikersnaam en de hashwaarde van het paswoord gewoon op in de databank. Bij het inloggen moeten we gewoon het volgende controleren:
  + Naam == naam in databank?
  + Hash(paswoord) == hashwaarde in databank?
  + De organisatie heeft de paswoorden zelf dus NIET in zijn databank staan en kan ze dus zelf NIET zien
  + Als iemand in de databank geraakt, kan hij de paswoorden NIET uitlezen → VEILIG!

Salting:

* Een extra maatregel om hashing veiliger te maken
* Wanneer 2 gebruikers hetzelfde paswoord gebruiken, zal voor beiden dezelfde hashwaarde worden opgeslagen. Hierdoor weten aanvallers dat ze door 1 paswoord te kraken 2 vliegen in 1 klap slaan
* Een salt is een random reeks bits dat wordt toegevoegd aan het paswoord. Zo zullen beide gebruikers een verschillende hash krijgen, ook al gebruiken ze hetzelfde paswoord

Rainbow tables:

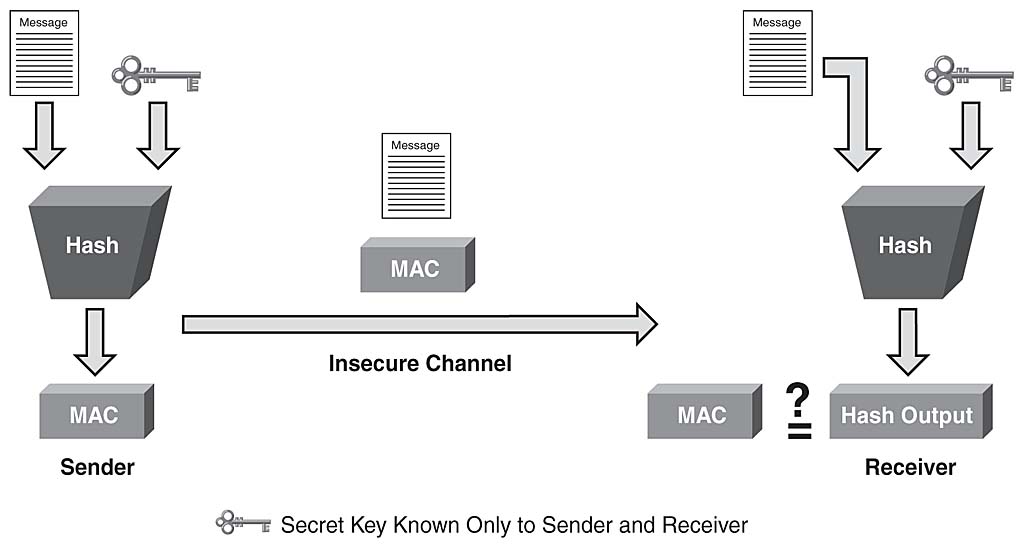
* Vanuit een hashwaarde de oorspronkelijke input berekenen is zo goed als onmogelijk
* Een manier is voor alle mogelijke inputwaarden de hashfunctie uit te rekenen (bruteforcing) en de resultaten opslaan in een lijst. Een dergelijke lijst noemt een Rainbow table
* Gebruik dus een aparte salt bij elk opgeslagen paswoord, dit maakt de Rainbowtable nutteloos

Collisions:

* Hashing algoritmes moeten telkens een unieke output hebben voor verschillende inputs
* Wanneer je voor 2 verschillende input waarden dezelfde output waarde krijgt, spreekt men van een “collision”
* Een hashing algoritme verliest zijn nut als collisions bewust veroorzaakt kunnen worden
* Hashing algoritmes worden zo onderverdeeld in zwakke en sterke hashing algoritmes
  + MD5 en SHA-1 zijn niet meer bruikbaar voor cybersecurity doeleinden, gebruik deze dus hiervoor NOOIT!
  + SHA-2 en SHA-3 kunnen wel nog gebruikt worden voor cybersecurity doeleinden

HMAC:

* HMAC versterkt het hashing algoritme door het toevoegen van een extra sleutel • Hierdoor wordt controleren van integriteit aangevuld met authenticatie
* De checksum is het resultaat van het HMAC-algoritme en wordt meegestuurd met het bericht
* De sterkte van HMAC hangt af van het gebruikte hashing algoritme (verschillende hashing algoritmes zijn mogelijk)



Vertragende hashing algortimes:

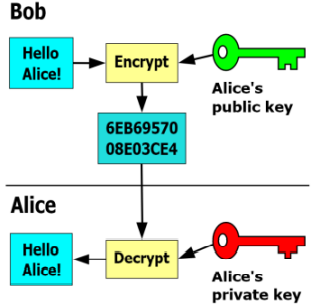
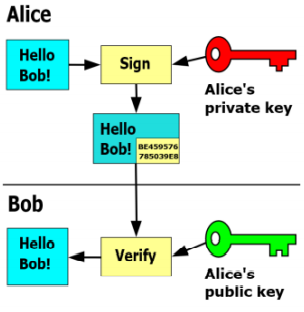
* Om te vermijden dat er heel veel pogingen worden gedaan om een hash te kraken of een collision te vinden wordt er vaak gebruik gemaakt van vertragende hashing algoritmes
* Een aanvaller met meer rekenkracht moet zo toch nog steeds lang wachten om de hashwaarde te kraken
* Bekende voorbeelden:
  + PBKDF2
  + bcrypt
  + Argon2

## 5.2 Digitale handtekeningen

* Digitale handtekeningen zijn zoals handtekeningen maar dan voor elektronische bestanden
* Hiermee kunnen 2 zaken worden gecontroleerd:
  + Het bestand is niet verandert nadat de handtekening is gegenereerd
  + Het bestand is daadwerkelijk afkomstig van de persoon die de handtekening heeft gegenereerd
* In veel landen heeft de elektronische handtekening als een traditionele analoge handtekening

Hoe werkt dit?

* Asymmetrische cryptografie genereert een publieke en private sleutel per persoon. Deze sleutels zijn wiskundig aan elkaar gelinkt



Voorbeeld sleutel:



## 5.3 Certificaten

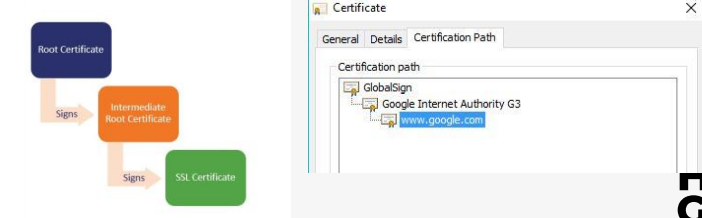
* Een digital certificaat is gelijkaardig aan een elektronisch paspoort
* Het laat gebruikers, toestellen en organisaties toe om veilige informatie te delen over het internet
* Een certificaat authenticeert en verifeert dat de verzender van bericht daadwerkelijk die persoon is
  + Koppelt een persoon aan een publieke sleutel
* Certificaten worden uitgedeeld door betrouwbare organisaties
* Certificaten bieden ook vertrouwelijkheid aan door encryptie

Gebruik bij werbsites:

* HTTPS versleutelt data tussen webserver en client
  + Hoe weet ik dat ik de website van de juiste webserver haal?

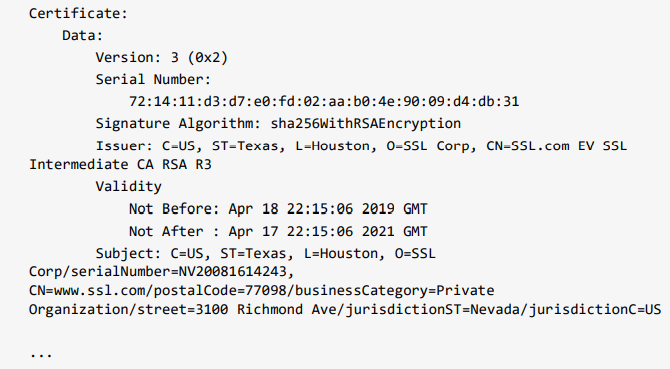


* Elke browser heeft een lijst van vertrouwde organisaties (Root Certificate Authorities)
* Organisaties bewijzen aan een Root CA dat ze te vertrouwen zijn en het internetdomein bezitten (bv. example.com)



Opstellen van een certificaat:

* Een digitaal certificaat volgt een gestandaardiseerd formaat zodat software dit kan lezen en verstaan, ongeacht de verzender
* De X.509 standaard is op dit moment de standaard voor het opstellen en beheren van digitale certificaten
* Een Public Key Infrastructure (PKI) is de verzameling van beleid, functies en procedures om certificaten te bewaren, beheren, verspreiden, gebruiken en ongeldig te verklaren
* Vb certificaat:



# 6. Het 5x9 principe

## 6.1 Hoge beschikbaarheid

Het 5x9 principe:

* The five nines
* Systemen en services kennen een uptime van 99,999%
* Downtime bedraagt 5,26 min per jaar
* Hoge beschikbaarheid kan je bekomen door:
  + Single points of failure vermijden
  + Robuuste systemen bouwen
  + Monitoren van de systemen
  + Failures / problemen detecteren wanneer ze zich voordoen.
  + Redundancy en backups

Omgevingen met hoge beschikbaarheid:

* Financiële sector:
  + Trading, diensten beschikbaar voor klant, vertrouwen van de klant
* Gezondheidssector:
  + Patiëntenzorg de klok rond
* Industrie
  + Fabrieken, assemblage, …
* Transportsector:
  + NMBS, luchtvaart, …
* Openbare veiligheid:
  + Staat in voor de veiligheid van de gemeenschap (brandweer, politie, leger, …)
* Nutsvoorzieningen:
  + Energiecentrales, waterzuiveringsstations, …
* Telecomsector:
  + Telefoon, internet, TV, …
* Retail industrie:
  + Supply chains, leveren van producten, …
  + Denk aan de eindejaarsperiode

Bedreigingen van de hoge beschikbaarheid:

* System failure
* Niet-doelbewuste oorzaak
* Doelbewuste aanval
* Natuurramp

## 6.2 Maatregelen om de beschikbaarheid te verbeteren

Assets management:

* Omvat het beheren van al deze assets (= bezittingen, eigendom)
* Er dient een volledig overzicht te zijn van alle hard- en software want deze moeten namelijk beveiligd worden
* Bedrijf kan dan een inschatting maken welke beveiligingsgevaren er zijn
* Volgende zaken worden in beschouwing genomen:
  + Elk hardware systeem
  + Elk besturingssysteem
  + Elk hardware netwerk toestel
  + Elk network device operating system
  + Elke softwareapplicatie
  + Elke firmware
  + Alle language runtime environments
* Sommige bedrijven kiezen voor een automatische inventarisatie:
  + Software die automatisch deze zaken bijhoudt.
* Asset classificatie:
  + Groepeer alle resources van een organisatie op basis van gemeenschappelijke kenmerken. Organisaties moeten documenten, datarecords, bestanden, schijven, etc. gaan classificeren.
* Identificatie van de bedreiging:
  + De United States Computer Emergency Readiness Team (US-CERT) en het U.S. Department of Homeland Security hebben een overzicht van vaak voorkomende kwetsbaarheden: common vulnerabilities and exposure (CVE). De CVE-identificatie geeft meer informatie over deze kwetsbaarheden.
* Risk Analysis:
  + Het proces om een inschatting te maken van gevaren van zowel natuurlijke of menselijke invloeden.
* Mitigation:
  + Het verminderen van het risico of het verkleinen van de kans op een aanval. Een aantal technische zaken om het risico te verminderen zijn bvb. gebruiken van authenticatie, rechten op bestanden instellen, het gebruiken van een firewall, etc.

Een diepe verdediging:

* Een verdediging in lagen:
  + Meerde barrières gaan maken
  + Als cybercriminelen de eerste laag kunnen binnendringen is er nog altijd de tweede laag en eventueel ook een derde

Zorgt dat je de cybercrimineel vaak een stap voor bent, je vermijdt dus het risico op een gelsaagde aanval

* Het beperken van toegang tot informatie:
  + Werknemers hebben alleen toegang tot de informatie die zij nodig hebben om hun job juist uit te voeren
  + Vermindert de kans op een aanval
* Diversiteit:
  + Varieer in manieren van beveiliging
  + Bv: in elke laag een ander encryptie algoritme
* Obscuring of verduisteren van informatie:
  + Bv: een organisatie geeft niet prijs welke OS-versie of welk type firewall er gebruikt wordt
* Simplicity of eenvoud:
  + Als de beveiliging te complex wordt, leidt dit meestal tot fouten.
  + Hogere beschikbaarheid

Redundantie:

* Single point of failure moet vermeden worden.
  + De zwakke schakels die ervoor kunnen zorgen dat een volledig systeem faalt.
  + Oplossing: niet op 1 element vertrouwen: redundantie inbouwen om kritische processen over te nemen op het moment dat er eentje faalt
* N + 1 redundantie:
  + Zorgt ervoor dat systemen beschikbaar blijven als er eentje faalt
  + Componenten (N) moeten steeds minimum 1 back-up component hebben (1)
  + Vb: een auto heeft steeds een reservewiel in de auto

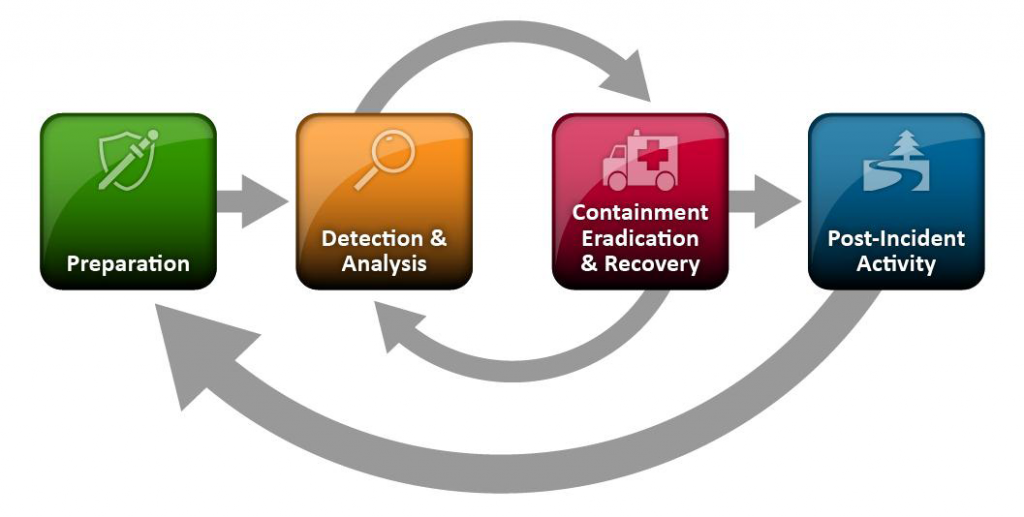
Weerstand van het system:

* Manieren voor systemen om te zorgen dat deze systemen een hoge tolerantie hebben voor falen
* Bv: routing protocols zorgen voor een verhoogde weerstand in een netwerk

## 6.3 Incident response

Incident response:

* Een aantal procedures die bedrijven hanteren om te reageren wanneer een buitengewoon event plaatsvindt
* Bedrijven moeten incident response plannen opstellen om voorbereid te zijn op het ergste:
* Omvat 4 fasen:
  + Voorbereiding: planning opstellen voor mogelijke gebeurtenissen
  + Detectie en analyse: het ontdekken van zo een gebeurtenis
  + Isoleren, uitdoven en herstellen: inspanningen doen om de gebeurtenis te isoleren, eventueel stoppen of uit doven en dan ook de opgelopen schade trachten te herstellen
  + Post-incident follow-up: nagaan hoe dit is kunnen gebeuren en bekijken hoe dit in de toekomst kan vermeden worden



Incident response technologie:

* Network Access Control (NAC):
  + Geeft toegang aan gebruikers tot een netwerk, als zij volledig voldoen aan de policy requirements van de organisatie.
  + Bv: het NAC-systeem eist als toestellen verbinden met het netwerk dat er een antivirus is geïnstalleerd
* Intrusion Detection Systems (IDSs):
  + Monitort het netwerkverkeer.
  + Luisteren naar hackpogingen en ongeautoriseerde toegang.
  + Het rapporteert, maar onderneemt geen actie.
* Intrusion Prevention Systems (IPSs):
  + Wordt op het pad tussen de bron en bestemming geplaatst.
  + Het detecteert onmiddellijk een netwerkprobleem en pakt het ook aan.
  + Wordt vaak meteen na de firewall geplaatst
* Advanced Threat Intelligence:
  + helpt organisaties om een cyberaanval te detecteren tijdens één van de fases (en soms zelfs voor de aanval plaatsvindt mits de juiste informatie).

## 6.4 Disaster recovery

Soorten rampen:

* Nattuurramp:
  + Geologische rampen (bvb. aardbevingen)
  + Meteorologische rampen (denk aan bliksem, hagel, tornado, …)
  + Gezondheidsramp (pandemieën, quarantaines)
  + Overige rampen (waterlek → overstroming, brand, …)
* Ramp veroorzaakt door mensen:
  + Gebeurtenissen op het werk (staking, ontslag, en bewust trager werken)
  + Socio-politieke events (vandalisme, blokkades protesten, sabotage, terreur, …)
  + Onderbreking in nutsvoorzieningen (stroom, communicatie, …)

Disaster recovery planning:

* Er is nood aan continuïteit bij een onderneming
  + Organisaties moeten plannen klaar hebben als het noodlot toeslaat
* Enkele zaken om te overwegen:
  + Documenteren van de configuraties
  + Zorgen voor alternatieve communicatiekanalen
  + Stroomvoorzieningen failsafe maken
  + Nagaan wat de impact voor de applicaties zijn
  + Nagaan hoe geautomatiseerde taken (tijdelijk) handmatig kunnen overgenomen worden
* Best practices:
  + Stel een policy op met richtlijnen om de continuïteit op verschillende vlakken te garanderen en maak een lijst met taken om deze richtlijnen uit te voeren.
  + Ga na welke kritieke systemen en processen er zijn binnen de organisatie. Prioriteer deze lijst op basis van noodzakelijkheid.
  + Identificeer de mogelijke kwetsbaarheden, bedreigingen en bereken de risico’s
  + Identificeer en implementeer controles en tegenmaatregelen om deze risico’s te beperken
  + Voorzie manieren om de kritieke systemen terug up and running te krijgen
  + Voorzie procedures om de organisatie ook draaiende te houden tijdens een chaotisch moment (bijvoorbeeld een ramp).
  + Test de plannen!
  + Actualiseer regelmatig deze plannen

## 6.5 verkenning en enumeratie

Hacking fasen:



### 6.5.1 Verkenningsfase:

* EN: Reconnaissance
* Passieve verkenning (bvb. website bezoeken)
  + Geen directe interactie met het target
* Actieve verkenning (bvb. bedrijf opbellen, naamkaartje vragen, ...)
  + Directe interactie met het target
  + Kan een spoor achterlaten
* Zonder authenticatie
* (Passieve) verkenning = niet illegaal
  + Vb. bezoeken van de webpagina van een bedrijf en kijken naar de vacatures.
* Technieken:
  + Social engineering
  + WHOIS db
  + nslookup
  + Dumpster diving

Verkenning:

* Research doen
* Ook wel footprinting genoemd
* Zo veel mogelijk informatie inwinnen over het target, zonder dat men ontdekt wordt
* Elementaire informatie (website, welke webserver, fysieke locaties, management, branch offices, nieuwsartikels, …)
* OS, Web servers & platformen (Windows versie, Apache, merken, ...)
* Queries uitvoeren om onderliggende infrastructuur te snappen (bvb. hosting, DB, …).
* Nadenken over kwetsbaarheden (men kent nu de versies)
* Target / organisatie begrijpen
* Beperken van aanvalsdomein (beperkte IP-range, beperkt aantal toestellen, …), op basis van ingewonnen informatie
* Vaak wordt een informatie DB opgesteld → verzamelen van ontdekte informatie – Wordt ook gebruikt om te prioriteren
* Layout van het netwerk maken (IP-adres ranges, DMZ, firewalls, …)

Types van verkenning:

* Passief
  + Publieke informatie gebruiken (geen direct contact met target)
  + Zowel online als offline bronnen (bvb. nieuws artikels)
  + Bvb. bedrijfswebsite gebruiken, welke manier van inloggen, …
* Actief
  + Direct contact met target (vaak social engineering)
  + Bvb. gebouw fysiek verkennen of solliciteren voor een job of het gebruiken van een

nmap tool om het target te scannen

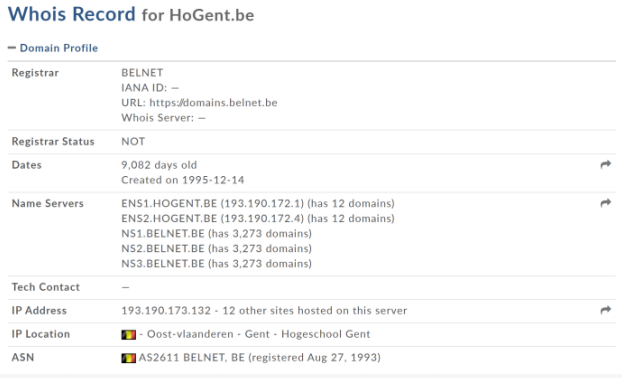
* Anoniem
  + Informatie vergaren van bronnen die niet kunnen achterhalen ie je bent
* Organisatie
  + Bvb. email van het bedrijf

Doel van verkenning:

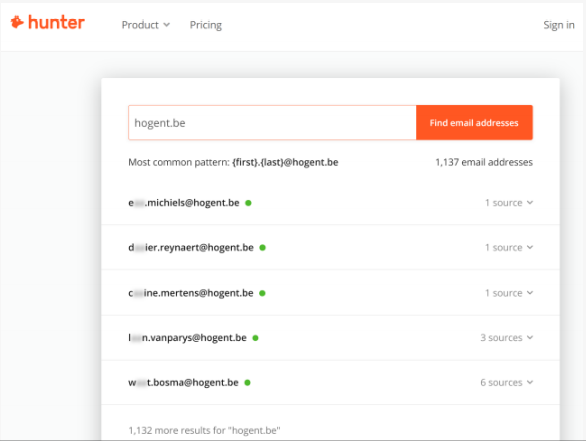
* Welke informatie zoekt men?
  + Organisatie:
    - Website (incl. broncode)
    - Organigram
    - Details van werknemers (incl. publieke informatie op social media); evt. voor wachtwoorden
    - Locaties van branches
    - Recent verhuisd?
    - Security policies (werd het personeel getraind?)
    - Nieuwsartikels
  + Netwerkinformatie:
    - Domeinnamen (incl. subdomeinen)
    - Interne domeinnamen (bvb. .com en .net)
    - IP-adressen (website, range, …)
    - TCP/UDP services
    - VPN-informatie
    - Intrusion Detection System
    - Telefoonnummers / VOIP
  + OS-informatie:
    - Gebruikers- & groepsnamen
    - Routing table
    - SNMP
    - Systeemarchitectuur (laatste updates?)
    - Remote access?
    - BYOD?

Tools voor verkenning:

* Zoekmachines (niet enkel de eerste 3 pagina’s)
* Websites (incl. subdomeinen)
* Applicaties / built-in commando’s
  + Nslookup
  + Powershell commands
* WHOIS:
  + Domein naam informatie (IP adres, eigenaar, ..)



* Hunter:
  + Emailadressen vinden

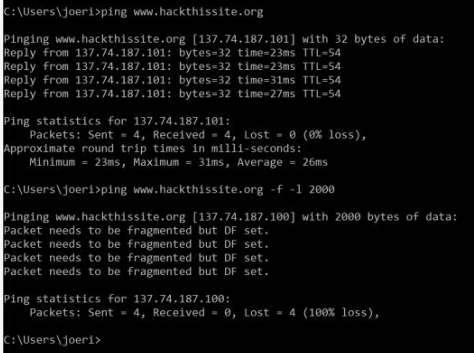


Website analyseren:

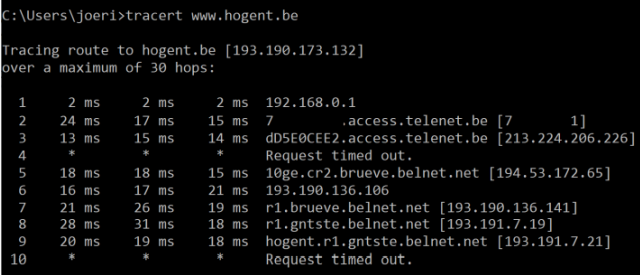
* Tools:
  + Netcraft.com
  + Builtwith.com
* Geeft informatie:
  + Frameworks,
  + DNS,
  + CDNs
  + Web stats
  + Hosting geschiedenis

### 6.5.2 Scanningsfase:

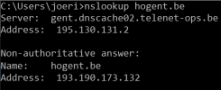
* Actieve scanning (bvb. ping sweep)
* Passieve scanning (bvb. netwerk sniffer -> netwerk afluisteren)
* Doel = informatie vergaren
  + OS-versies van toestellen
  + Hardware toestellen (routers, firewalls, )
  + IP addres schema (bvb. printers, werknemer PC’s, …)
  + Kwetsbaarheden (bvb. versies – zero day attacks)
* Technieken:
  + Poort scanner
  + Vulnerability scanners
  + Trace route
* Vaak voorkomende types scans:
  + Port Scanning:
    - Detecteren van open poorten en services die draaien op het target.
    - Vertrekpunt om na te gaan welke services en applicaties er luisteren naar bepaalde poorten
  + Network Scanning:
    - IP addressen, Operating system details, Topology details, trusted routers information, etc
    - Doel: het vinden van issues in het target netwerk opdat de klant/opdrachtgever zijn/haar netwerk kan verbeteren.
  + Vulnerability scanning:
    - Gekende kwetsbaarheden of zwaktes scannen
    - Doel: het vinden van kwetsbaarheden voor de specifieke applicaties en services die op het netwerk aanwezig zijn
* PING:
  + Commando:
    - Ping \*url\*
  + IP-adres
  + Pakketgrootte
  + Buffer
  + Wordt soms geblokkeerd



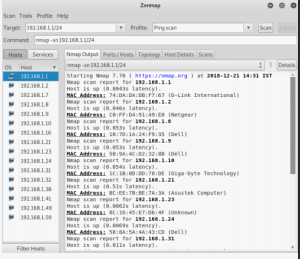
* Trace Route
  + Commando (windows): tracert \*url\*
  + Route die de request aflegt
  + Hops die men onderweg tegenkomt worden getoond
  + Soms worden requests geblokkeerd door een hop



* Nslookup (DNS):
  + Commando: nslookup \*url\*
  + Geassocieerde IP-adressen
  + Verschillende gegevenstypes
    - MX (Mail eXchange records)
    - CNAME (canonical name record)
  + Via nslookup kunnen we achterhalen wat het IP-adres van de server is, wat de domeinnaam is, wat de domeinnaam en IP-adres van de mailserver zijn, etc.
  + DNS wordt o.a. gebruikt om een domeinnaam (bvb. Google.com) om te zetten naar een IP adres.



* Nmap:
  + Bestaat al sinds 1997
  + Voluit: network mapper
  + Is een populaire netwerkscanner
  + Wordt ook gebruikt als port scanner
  + Wordt gebruikt om het netwerk in kaart te brengen en is enorm populair.
  + Heeft ook een grafische user interface: Zenmap



* Poort scanner:
  + Een poort scanner kan gebruikt worden om het netwerk onder de loep te nemen en (binnen een bereik) te scannen naar open poorten.
  + Een poort die open staat kan gezien worden als toegangspoort.
  + Wanneer een applicatie of service over het netwerk communiceert doet het dit via een poort. Een poort wordt geassocieerd met en gereserveerd voor die bepaalde service of applicatie. Communicatie dat langs die poort passeert, wordt dan doorgestuurd naar de applicatie of service. Wanneer een poort open staat, kan deze als een toegangspoort gebruikt om toegang te krijgen tot het netwerk en tot de applicatie of service.

Enumeratie:

* Komt na het scannen, maar houdt er wel mee verband
* Welke services draaien er?
* En ook: op welke versies draaien deze services?
* Je vergaart meer informatie dan enkel IP-adressen en poorten: gebruikersnamen, netwerk shares, software en versie van de services, …
* Kan via nmap commando
* Deze informatie kan men dan opnieuw gaan gebruiken in een latere fase.
* Informatie in deze stap:
  + Network resources en shares
  + Gebruikersnamen en groepen (denk aan Active Directory)
  + Routing tables
  + Auditing en service settings
  + Namen van de toestellen
  + Applicaties
  + SNMP en DNS details
* Netwerk mappen kan bvb. via deze tools:
  + LanState pro:
  + PRTG Network Monitor
  + Je moet wel eerst toegang hebben tot het netwerk.

# 7. Het beschermen van een ICT-omgeving

## 7.1 Systemen en apparaten beschermen

Host hardening:

* Beveiliging van het besturingssysteem
  + Standaardconfiguratie aanpassen
  + Verwijderen onnodige software
  + Beveiligingspatches en updates
* Installeren antimalware
  + Bescherming tegen virussen, worms, keyloggers, spyware, …
  + Mobiele apparaten zijn ook kwetsbaar!
  + Let op met gratis software: frauduleuze antimalware kan zelf malware bevatten
* Beheer van patches (= code-updates)
  + Kunnen centraal beheerd worden
  + Servicepack:
    - = uitgebreide update-applicatie
    - Beschikbaar gesteld door fabrikant
    - Combineert verschillende patches en upgrades
* Host-gebaseerde Firewall
  + Regelt inkomend en uitgaand netwerkverkeer
  + Uitgevoerd op host-computer
* Host Intrusion Detection System (HIDS)
  + Controleert verdachte activiteiten
  + Uitgevoerd op host-computer
* Configuratie van een Virtueel Privaat Netwerk (VPN)
  + Beveiligde communicatie over publiek netwerk
  + Maakt privénetwerk aan tussen verschillende fysieke locaties
    - Verbinding branch office en main office
    - Gebruikers kunnen van thuis aan IT-diensten binnen bedrijfsnetwerk

Draadloze en mobiele apparaten:

* WEP - Wired Equivalent Privacy
  + Basisbescherming WiFi
  + 10 tot 26 hexadecimale karakters (40 – 104 bits)
  + Niet (meer) veilig!
* WPA / WPA2 - Wi-Fi Protected Access
  + Grote verbetering ten opzichte van WEP
  + Gebaseerd op AES
  + Tegenwoordig is WPA2 de standaard
* Toevoegen wederzijdse authenticatie:
  + Voorkomt man-in-the-middle aanval (rogue access point)
  + Authenticatie tussen beide entiteiten

Bescherming van (host) data:

* Bestandstoegangscontrole
  + Machtigingen op bestanden en mappen
  + Ingesteld per gebruiker of groep gebruikers
* File encryption
  + Encrypteren van gevoelige data
  + Kan op individuele bestanden of op hele harde schijf
* Systeem- en gegevensback-ups
  + Reservekopie van gevoelige data
  + Typisch op verwijderbare media (bv. tape drive)

Content control:

* Content screening en blokkering
  + Beperkt de inhoud waartoe een gebruiker toegang heeft met een webbrowser via internet.
  + Kan bepaalde sites blokkeren:
    - Pornografie
    - Controversiële religieuze of politieke inhoud
    - Social media (nuttig in bedrijfsomgevingen)

Disk cloning en deep freeze:

* Software om systeem te herstellen naar standaardstatus
  + Beschermen besturingssysteem en configuratiebestanden
  + Disk clone
    - de inhoud van de harde schijf van de computer naar een afbeeldingsbestand (image file, bv ISO) gekopieerd.
  + Deep freeze
    - “Bevriest” de partitie van de harde schijf
    - Wanneer een gebruiker het systeem opnieuw opstart, keert het systeem terug naar de bevroren configuratie
    - Alle wijzigingen door gebruiker verloren bij herstarten
    - Vooral nuttig voor publieke toestellen (bv. internetcafé, bibliotheek)

Fysieke bescherming:

* Beveiligingskabels en sloten
  + Kabelsloten
  + Belangrijke apparatuur in afgesloten ruimte
  + Veiligheidskooien rond apparatuur
* Logout timers
  + Toestel automatisch vergrendelen na periode van inactiviteit
  + Indien niet: systeem kwetsbaar voor onbevoegde gebruikers die een aanstaande laptop zien
* Beperken inlogtijden
  + Blokkeren login buiten kantooruren
* GPS-tracking
  + Mobiel toestel terugvinden bij diefstal of verlies
  + Maakt gebruik van gps-satellieten
* Inventaris en RFID-tags
  + Radiofrequentie-identificatie gebruikt radiogolven
  + Gebruikt om object te identificeren en volgen
  + Inventaris houdt tags bij

## 7.2 Server Hardening

Beveiligde toegang op afstand:

* Externe toegang
  + Laat toe dat gebruikers op afstand toegang hebben tot een lokaal intern netwerk.
* Telnet
  + Verouderd
  + Data (o.a. login en wachtwoord) verzonden in plaintext
  + Niet veilig!
* SSH
  + Opvolger Telnet
  + Een protocol dat een veilige (gecodeerde) beheerverbinding biedt met een extern apparaat.
  + Encryptie van data
* SCP
  + Veilige overdracht van bestanden naar extern systeem
  + Maakt onderliggend gebruik van SSH (authenticatie + bescherming van data in beweging)

Administratieve maatregelen:

* Poorten en services beveiligen
  + Via open poorten kunnen cybercriminelen achterhalen welke services er draaien op een host
  + Op veel systemen draaien meer services dan nodig
  + Beheerder moet elke service bekijken en nagaan of deze noodzakelijk is, alsook de mogelijke risico’s inschatten
* Geprivilegieerde accounts
  + Geprivilegieerde accounts zijn krachtigste accounts
  + Beheerders gebruiken deze accounts om besturingssystemen, applicaties en netwerkapparaten te implementeren en te beheren
  + Hebben vaak verhoogde of zelfs onbeperkte toegang
  + Beheerder moet deze accounts voldoende beveiligen of eventueel verwijderen om risico’s te beperken
* Group Policies
  + Onderdeel van Active Directory
  + Voor gebruik in Windows omgeving
  + Laat toe om bepaalde veiligheidsmaatregelen in te stellen voor een groep gebruikers
    - Bv. Password policy, vergrendelingsbeleid, toegang tot bronnen, …
    - Zie ook Windows Server I en II (2e en 3e bachelor)
* Logboeken en waarschuwingen
  + Een logboek registreert gebeurtenissen op een systeem
  + Bevatten uitgebreide informatie voor elke gebeurtenis
  + Belangrijk voor computerbeveiliging (AAA: accounting)

Fysieke bescherming van een server:

* Stroomvoorziening
  + Cruciaal bij beschermen van informatiesystemen
  + Continue levering noodzakelijk voor server- en gegevensopslagfaciliteiten
* Verwarming, ventilatie en airconditioning (HVAC)
  + Zijn cruciaal voor de veiligheid van mensen en informatiesystemen
  + Regelen de omgeving (temperatuur, vochtigheid, luchtstroom en luchtfiltering)
* Hardware monitoring
  + Vaak aangetroffen in grote server farms
  + Een server farm is een faciliteit die honderden of duizenden servers voor bedrijven huisvest

## 7.3 Netwerk Hardening

Netwerkapparaten beschermen:

* Network Operations Centers (NOC)
  + Op één of meerdere locaties
  + Bieden gedetailleerde status van netwerk
  + Ground zero voor oplossen van netwerkproblemen, prestatiebewaking, softwaredistributie en updates, communicatiebeheer en apparaatbeheer
* Netwerkswitches
  + Hart van het moderne netwerk
  + Kwetsbaar voor diefstal, hacking en toegang op afstand
  + Doelwit voor aanvallen op netwerkprotocollen of DOS aanvallen
* VLANs (virtuele netwerken)
  + Bieden manier om apparaten binnen netwerk (LAN) logisch te groeperen
  + Bv. VLAN 1 voor studenten, VLAN 2 voor docenten, …
* Firewalls
  + Hardware- of software die netwerk beveiligen
  + Voorkomt dat ongeautoriseerd of potentieel gevaarlijk verkeer het netwerk binnenkomt
* Routers
  + Link tussen verschillende netwerken
  + Communiceren met elkaar om het beste pad te bepalen
  + Gebruiken routeringsprotocollen om routeringsbeslissingen te nemen
* Draadloze en mobiele apparaten
  + Bieden mobiliteit en gemak
  + Brengen tal van kwetsbaarheden met zich mee
    - Diefstal, hacking en ongeautoriseerde toegang op afstand, sniffing, man-in-the-middle-aanvallen en aanvallen op prestaties en beschikbaarheid
* Netwerk- en routingservices
  + Cybercriminelen gebruiken kwetsbare netwerkservices om een apparaat aan te vallen of om het te gebruiken als onderdeel van de aanval
  + Het beveiligen van netwerkservices zorgt ervoor dat alleen de noodzakelijke poorten zichtbaar en beschikbaar zijn
  + Netwerkdiensten omvatten; DHCP, 21 DNS, ICMP, Routing Services (RIP-OSPF-ISS), NTP en andere

Spraak- en videoapparatuur:

* Voice over IP (VoIP): telefoneren via internet
* Camera’s:
  + Gebruikt voor beveiliging en voor videobellen
  + Een internetcamera verzendt en ontvangt gegevens via een LAN en / of internet. Een gebruiker kan op afstand live video bekijken met een webbrowser op een breed scala aan apparaten
* Videoconferentieapparatuur:
  + Speciale hardware voor videoconferenties
* Netwerk- en IoT-sensoren:
  + Slimme apparaten en sensoren
  + Hart van het Internet of Things (IoT)
  + Processen automatiseren, omgevingen monitoren, gebruiker waarschuwen voor ongunstige omstandigheden

## 7.4 Fysieke beveiliging

Fysieke toegangscontrole:

* Omheiningen en barricades
  + Buitenste beveiligingslaag
  + Omheining, beveiligingspoorten, slagbomen, bewakers, …
* Biometrie
  + Geautomatiseerde methoden om persoon te herkennen
  + Op basis van een fysiologisch of gedragskenmerk
  + Gezichtsherkenning, vingerafdruk, irisscan, stemherkenning, …
  + Kunnen basis vormen voor zeer veilige authenticatie
* Badges en toegangslogboeken
  + Een badge geeft een persoon toegang tot een gebied of ruimte
  + Toegangsbadges maken gebruik van verschillende technologieën, zoals een magneetstrip, streepjescode of biometrie
  + Het systeem registreert de transactie zodat deze later kan worden opgehaald
  + Rapporten laten zien wie op welk tijdstip toegang vroeg

Bewaking:

* Bewakers en escorts
  + Fysieke toegangscontroles zijn afhankelijk van personeel om in te grijpen en de daadwerkelijke aanval of indringing te stoppen
  + Bewakers kunnen toegang tot gevoelige gebieden controleren
* Videobewaking en elektronische bewaking
  + Kan beveiligingspersoneel aanvullen of in sommige gevallen vervangen
  + Mogelijk om gebieden te bewaken zonder bewakers of personeel
  + Video’s kunnen gedurende lange periodes bewaard worden
  + Mogelijkheid tot bewegingsdetectie en bijhorende meldingen
* RFID en draadloze bewaking
  + Gebruikt om belangrijke informatiesystemen te beheren en te lokaliseren

# 8. Werken als een cybersecurity-specialist

## 8.1 De verschillende cybersecurity domeinen

Het gebruikersdomein:

* Omvat de gebruikers die toegang hebben tot de data van een organisatie

Bv. werknemers, klanten, onderaannemers, ...

* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Gebruikers zijn vaak de zwakste schakel voor cybersecurity en vormen een aanzienlijke bedreiging
* Beheer van bedreigingen:
  + Geef training en opleidingen voor cybersecurity bewustzijn
  + Zorg voor automatische filtering op inhoud en het scannen van antivirusprogramma’s
  + Schakel CD- en USB-stations uit
  + Minimaliseer machtigingen, beperk de toegang, hou gebruikers in de gaten en schakel inbraakdetectie in

Het Toesteldomein:

* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Onbewaakte toestellen (bv. even naar de WC), downloads van gebruikers, niet up-to-date software
  + Malware, gebruik van ongeautoriseerde media en overtredingen van het beleid voor aanvaardbaar gebruik van toestellen

Het LAN-domein:

* Local Area Network (LAN)
* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Onbevoegde toegang tot het netwerk, systemen, applicaties, data, ...
  + Kwetsbaarheden in software, foute configuraties, niet up-to-date software
  + Ongeautoriseerd netwerkonderzoek en scannen van poorten

Het private cloud domein:

* Wide Area Network (WAN)
* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Onbevoegd netwerkonderzoek, scannen van poorten en toegang
  + Kwetsbaarheden of foute configuratie in de software van routers, firewalls en besturingssystemen
  + Gebruikers op afstand die inloggen op de infrastructuur van de organisatie en gevoelige informatie downloaden

Het publieke cloud domein:

* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Datalekken, verlies of diefstal van intellectuele eigendommen, en gelekte of gekraakte inloggegevens
  + Federatieve identiteitsopslagplaatsen zijn een gegeerd doel
  + Kapen van accounts, social engineering en gebrek aan inzicht aan de kant van de organisatie

Het fysieke domein:

* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Natuurlijke bedreigingen zoals onweer, geologische bedreigingen (aardbeving, overstroming, ...) en elektriciteitsonderbrekingen
  + Onbevoegde toegang, diefstal, niet afgeschermd datacenter, gebrek aan bewaking
  + Social engineering, schending van de elektrische begrenzing

Het applicatiedomein:

* Veel voorkomende bedreigingen en kwetsbaarheden:
  + Onbevoegde toegang tot datacenters, computers, elektriciteitscabines
  + Server downtime voor onderhoud, IT-systemen zijn offline voor langere periodes
  + Kwetsbaarheden in het besturingssysteem voor netwerkapparatuur
  + Verlies van data

## 8.2 De ethiek van werk in cybersecurity

Ethiek en leidende principes:

* Ethiek:
  + Is de kleine stem in het achterhoofd dat zegt wat mag en wat niet, ongeachte het legaal is of niet
  + De organisatie vertrouwt de cybersecurity-specialist met zijn meest gevoelige data
  + De cybersecurity-specialist moet verstaan hoe wetgeving en de belangen van de organisatie helpen bij het nemen van ethische beslissingen
* Computer Ethics Institute (CEI)
  + Een bron voor het identificeren, beoordelen en reageren op ethische kwesties in de ICT-wereld
  + Een van de eerste organisaties ter wereld i.v.m. ethiek in de ICT-wereld
  + De ICT-wereld gaat razendsnel vooruit, daarbij komen steeds nieuwe ethische kwesties en problemen boven

Cyberwetten en aansprakelijkheid:

* Cybercrime (computermisdaad)
  + Wetten verbieden ongewenst gedrag
    - Er is wetgeving op Europees en Belgisch niveau
  + Wetten kunnen niet volgen op de actualiteit en vooruitgang in de ICT-wereld
  + Er zijn verschillende manieren waarop een toestel deel uitmaakt van computermisdaad
    - Misdaad geholpen door computersystemen
    - Misdaad gericht op computersystemen
    - Computerincidentele misdaad (bv. bij kinderporno is de computer een opslagmiddel en niet het middel of doelwit om de misdaad te plegen)
* Organisaties tegen computermisdaad
  + Er bestaan verschillende organisaties om computermisdaad te bestrijden
  + België: Federal Computer Crime Unit (FCCU), Centre for Cyber Security Belgium, ...
  + Wereldwijd: Europol, ENISA, Interpol, ...

Websites voor cybersecurity:

* National Vulnerability Database (NVD):
  + Een geautomatiseerde databank van kwetsbaarheden gehost door het NIST
* Computer Emergency Response Team (CERT):
  + Helpt overheden en organisaties met het beveiligen van softwaresystemen en netwerken
  + Bestuderen cybersecurity-problemen en ontwikkelen methodes en tools om deze tegen te gaan
* Internet Storm Center (ISC):
  + Host een waarschuwingsdienst over de cybersecurity-toestand van het internet
  + ISC werkt samen met ISP’s tegen cybercriminelen
  + Het ISC verzamelt per dag millioenen log entries van inbraakdetectiesystemen in meer dan 50 landen
* The Advanced Cyber Security Center (ACSC):
  + Een non-profit organisatie dat samenwerkt met overheden, academici en industry 16 om onderzoek te doen naar cybersecurity bedreiging en informatie uit te wisselen
  + Ook biedt het opleidingen aan om het beroep cybersecurity-specialist in de kijker te zetten
* Het is enorm belangrijk om op de hoogte te blijven van de laatste bedreigingen en verdedigingen

Cybersecurity wapens:

* Vulnerability scanners:
  + Onderzoekt computers, netwerken en programma’s naar kwetsbaarheden en geeft deze in een lijst met prioriteiten terug
* Penetrating testing:
  + Het testen of er zwakheden zijn in systemen door het gebruik van hacktechnieken
  + Een cybersecurity-specialist probeert een systeem te kraken zonder weet van gebruikersnamen, paswoorden of andere normale inlogmogelijkheden
* Packet analyzers (packet sniffers):
  + Onderscheppen en loggen netwerkverkeer.
  + Het toont de inhoud van elk verstuurd pakket op dat netwerk.
  + Dit kan zowel op bedrade als draadloze netwerken.
* Security tools:
  + Er zijn ontelbare security tools beschikbaar.
  + Het is de verantwoordelijkheid van de cybersecurity-specialist om te weten wanneer hij welke tool moet gebruiken en dit ook op de juiste manier doet

## 8.3 Cybersecurity profielen

Rollen:

* Ook defensie (de militaire inlichtingendienst, ADIV) werft af en toe Cybersecurity specialisten aan.
  + De dienst Cyber Security Operations Centre (CSOC) monitort en beveiligt de computernetwerken en wapensystemen van de Belgische krijgsmacht.
  + Beschermen van de militaire informatie.
  + Garanderen van de integriteit en de beschikbaarheid van de militaire netwerken en wapensystemen.
  + Cyberexpertise ontwikkelen voor het verwerven van inlichtingen en voor het ondersteunen en uitvoeren van militaire operaties.
  + De opdrachten worden anders ingevuld naargelang je specifieke rol.
* Vulnerability Assessor: neemt deel aan het risicobeoordelingsproces van de interne en externe ITomgevingen.
* Threat Analyst identificeer: verzamelt en analyseert informatie over dreigingen tegen het netwerk.
* Incident Handler: zoekt naar mogelijke aanvallen, door het doorzoeken van de beschikbare logs en van allerhande veiligheidsmeldingen.
* Digital Forensics Analyst: spitst zich volledig toe op het onderzoek van images van geheugen of harde schijven.
* Malware Analyst: voert gedetailleerde analyses uit van malware.

## 8.4 De volgende stap

Verken de inhoud van het werk van een cybersecurity-specialist:

* Het ISO-cybersecurity 27000 model vermeld verschillende soorten cybersecurity-functies:
  + Managers verantwoordelijk voor IT en beveiliging
  + Informatiebeveiligingsprofessionals
  + Beveiligingsmanager voor fysieke beveiliging
  + HR-contactpersoon voor opleidingen en disciplinaire maatregelen
  + Systeem- en netwerkbeheerders, beveiligingsarchitecten en andere IT-professionals