



# Cybersecurity

2020-2021

## 7. Het beschermen van een ICT omgeving



## **7. Het beschermen van een ICT omgeving**

7.1 Systemen en apparaten beschermen

7.2 Server Hardening

7.3 Netwerk Hardening

7.4 Fysieke beveiliging

**HO  
GENT**

**7.1**

# **Systemen en apparaten beschermen**

**HO  
GENT**

## 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

**HO  
GENT**

## Host Hardening

Het besturingssysteem speelt een cruciale rol bij de werking van een computersysteem en is het doelwit van veel aanvallen.

- Een beheerder versterkt een besturingssysteem door de standaardconfiguratie aan te passen om het beter te beveiligen tegen bedreigingen van buitenaf.
- Dit proces omvat het verwijderen van onnodige programma's en services.
- Een andere essentiële vereiste voor het versterken van besturingssystemen is de toepassing van beveiligingspatches en updates.

Daarnaast kan je op elk systeem antimalware installeren. Malware omvat virussen, wormen, Trojaanse paarden, keyloggers, spyware en adware.

- Ze schenden allemaal de privacy, stelen informatie, beschadigen het systeem of verwijderen en corrumperen gegevens.

- Het is belangrijk om computers en ook mobiele apparaten te beschermen met behulp van betrouwbare antimalwaresoftware.

## Host Hardening (cont.)

### Beheer van patches

- 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

### Host Intrusion Detection System (HIDS)

- Controleert verdachte activiteiten

**HO  
GENT**

## Host Hardening

### Beheer van patches

Patches zijn code-updates die fabrikanten bieden om te voorkomen dat een nieuw ontdekt virus of worm een succesvolle aanval uitvoert. Fabrikanten combineren patches en upgrades tot een uitgebreide update-applicatie, een servicepack genaamd.

### Host-gebaseerde firewalls

Een softwarefirewall is een programma dat op een computer wordt uitgevoerd om verkeer tussen de computer en andere aangesloten computers toe te staan of te weigeren. De softwarefirewall past een reeks regels toe op datatransmissies door inspectie en filtering van datapakketten.

### Host Intrusion Detection Systems

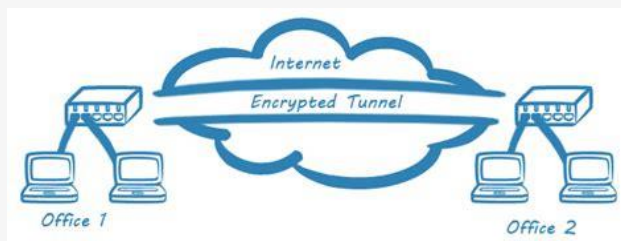
Een host inbraakdetectiesysteem (HIDS) is software die wordt uitgevoerd op een hostcomputer die verdachte activiteiten

controleert.

## Host Hardening (cont.)

Configuratie van een **Virtueel Privaat Network (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



**HO  
GENT**

### Host Hardening (cont.)

#### Beveiligde communicatie (VPN's)

Wanneer u verbinding maakt met het lokale netwerk en bestanden deelt, blijft de communicatie tussen computers binnen dat netwerk. Om te communiceren en bronnen te delen via een netwerk dat niet beveiligd is, gebruiken gebruikers een Virtual Private Network (VPN). Een VPN is een privénetwerk dat externe sites of gebruikers met elkaar verbindt via een openbaar netwerk, zoals internet.



## 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



**HO  
GENT**

## Draadloze en mobiele apparaten

### Wired Equivalent Privacy (WEP)

Eén van de belangrijkste componenten van moderne computers zijn mobiele apparaten. De meeste apparaten die in de huidige netwerken worden aangetroffen, zijn laptops, tablets, smartphones en andere draadloze apparaten. WEP is een van de eerste veelgebruikte Wi-Fi-beveiligingsstandaarden. De WEP-standaard biedt authenticatie- en coderingsbeveiliging.

### WPA/WPA2

De volgende grote verbetering van draadloze beveiliging was de introductie van WPA en WPA2. Wi-Fi Protected Access (WPA) was het antwoord van de computerindustrie op de zwakte van de WEP-standaard. De WPA-standaard zorgde voor verschillende beveiligingsverbeteringen.

### Wederzijdse authenticatie

Een aanvaller kan een man-in-the-middle-aanval lanceren die erg moeilijk te detecteren is en kan resulteren in gestolen inloggegevens en verzonden gegevens. Om malafide toegangspunten te voorkomen, ontwikkelde de computerindustrie wederzijdse authenticatie. Wederzijdse authenticatie, ook wel tweerichtingsauthenticatie genoemd, is een proces of technologie waarbij beide entiteiten in een communicatieverbinding met elkaar authenticeren.

## 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)

**HO  
GENT**

## Bescherming van (host) data

### Bestandstoegangscontrole

Dit bestaat uit machtigingen die de toegang tot mappen of bestanden beperken voor een individu of voor een groep gebruikers.

### File encryption

File encryption of bestands codering is een hulpmiddel dat wordt gebruikt om gegevens te beschermen die zijn opgeslagen in de vorm van bestanden. Versleuteling transformeert gegevens met behulp van een gecompliceerd algoritme om ze onleesbaar te maken. Softwareprogramma's kunnen bestanden, mappen en zelfs hele schijven versleutelen.

### Systeem- en gegevensback-ups

Een gegevensback-up slaat een kopie op van de informatie van een computer op verwijderbare back-upmedia. Een back-up maken van gegevens is één van de meest effectieve manieren om

gegevensverlies te voorkomen. Als de computerhardware uitvalt, kan de gebruiker de gegevens van de back-up herstellen nadat het systeem weer functioneel is.

## 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)
  - ...



**HO  
GENT**

### Content screening en blokkering (Content Control)

Content control software beperkt de inhoud waartoe een gebruiker toegang heeft met een webbrowser via internet.

Content control software kan sites blokkeren die bepaalde soorten materiaal bevatten, zoals pornografie of controversiële religieuze of politieke inhoud.

## Disk Cloning en Deep Freeze

- Software om systeem te herstellen naar **standaardstatus**
- Beschermen besturingssysteem en configuratiebestanden
- **Disk clone**
  - Image (bv. ISO) van volledige harde schijf
- **Deep freeze**
  - “Bevriest” de partitie van de harde schijf
  - Alle wijzigingen door gebruiker verloren bij herstarten
  - Vooral nuttig voor publieke toestellen (bv. internetcafé, bibliotheek)



**HO  
GENT**

### Disk Cloning en Deep Freeze

- Er zijn veel third-party toepassingen beschikbaar om een systeem terug te zetten naar een standaardstatus. Hierdoor kan de beheerder het besturingssysteem en configuratiebestanden voor een systeem beschermen.
- Met het klonen van schijven (disk cloning) wordt de inhoud van de harde schijf van de computer naar een afbeeldingsbestand (image file) 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. Het systeem slaat geen wijzigingen op die de gebruiker aanbrengt, dus alle geïnstalleerde applicaties of opgeslagen bestanden gaan verloren wanneer het systeem opnieuw wordt opgestart.

## 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

### Beperken inlogtijden

- Blokkeren login buiten kantooruren

**HO  
GENT**

## Fysieke bescherming

### Beveiligingskabels en sloten

Er zijn verschillende methoden om computerapparatuur fysiek te beschermen:

- Gebruik kabelsloten.
- Houd telecommunicatieruimten afgesloten.
- Gebruik veiligheidskooien rond apparatuur.

### Logout timers

Een werknemer staat op en verlaat zijn computer om een pauze te nemen. Als de medewerker geen actie onderneemt om zijn werkstation te beveiligen, is alle informatie op dat systeem kwetsbaar voor een onbevoegde gebruiker.

Medewerkers kunnen al dan niet uitloggen bij hun computer wanneer ze de werkplek verlaten. Daarom is het een goede beveiligingspraktijk om een inactieve timer te configureren die de gebruiker automatisch uitlogt en het scherm vergrendelt.

## Inlogtijden

In sommige situaties wil een organisatie dat werknemers zich tijdens bepaalde uren aanmelden, zoals van 07.00 uur tot 18.00 uur. Het systeem blokkeert logins tijdens de uren die buiten de toegestane inloguren vallen.



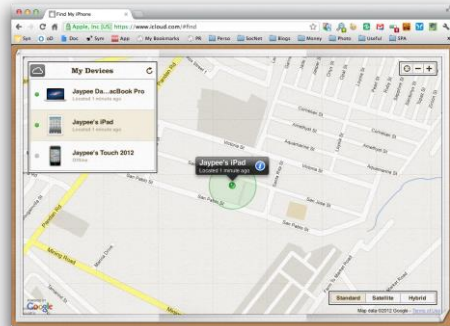
## Fysieke bescherming (cont.)

### 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



**HO  
GENT**

## Fysieke bescherming

### GPS-tracking

Gebruikt satellieten en computers om de locatie van een apparaat te bepalen. GPS-technologie is een standaardfunctie op smartphones die realtime positiebepaling mogelijk maakt. GPS-tracking kan een locatie binnen 100 meter lokaliseren.

### Inventaris en RFID-tags

Radiofrequentie-identificatie (RFID) gebruikt radiogolven om objecten te identificeren en te volgen. RFID-inventarisatiesystemen gebruiken tags die zijn bevestigd aan alle items die een organisatie wil volgen.

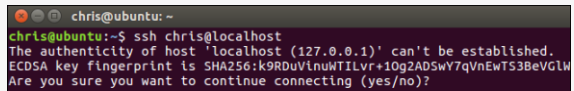
## **7.2 Server Hardening**

**HO  
GENT**

## 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
  - Encryptie van data
- **SCP**
  - Veilige overdracht van bestanden naar extern systeem
  - Maakt onderliggend gebruik van SSH (authenticatie + bescherming van data in beweging)



```
chris@ubuntu: ~  
chris@ubuntu:~$ ssh chris@localhost  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
ECDSA key fingerprint is SHA256:k9RDUvinuWILvr+10g2ADSwY7qVnEwTS3BeVGLW  
Are you sure you want to continue connecting (yes/no)?
```

**HO  
GENT**

## Beveiligde toegang op afstand

Externe toegang verwijst naar elke combinatie van hardware en software waarmee gebruikers op afstand toegang hebben tot een lokaal intern netwerk.

### Telnet, SSH en SCP

Secure Shell (SSH) is een protocol dat een veilige (gecodeerde) beheerverbinding biedt met een extern apparaat.

- **SSH** moet Telnet vervangen voor extern beheer.
- **Telnet** is een ouder protocol dat gebruikmaakt van onveilige, leesbare teksttransmissie van zowel de login authenticatie (gebruikersnaam en wachtwoord) als de gegevens die worden verzonden tussen de communicerende apparaten
- **Secure Copy (SCP)** draagt veilig computerbestanden over tussen twee externe systemen. SCP gebruikt SSH voor gegevensoverdracht (inclusief het authenticatie-element), dus SCP zorgt voor de authenticiteit en vertrouwelijkheid van de

gegevens 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
- Hebben vaak verhoogde of zelfs onbeperkte **toegang**
- Beheerder moet deze accounts voldoende **beveiligen** of eventueel **verwijderen** om risico's te beperken

**HO  
GENT**

## Administratieve maatregelen

### Poorten en services beveiligen

Cybercriminelen maken gebruik van de services die op een systeem worden uitgevoerd, omdat ze weten dat de meeste apparaten meer services of programma's uitvoeren dan ze nodig hebben. Een beheerder moet elke service bekijken om de noodzaak ervan te verifiëren en het risico ervan te evalueren. Verwijder onnodige services.

### Geprivilegieerde accounts

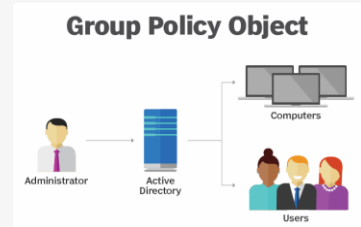
Cybercriminelen maken misbruik van geprivilegieerde accounts omdat dit de krachtigste accounts in de organisatie zijn. Bevoorrechte accounts hebben de inloggegevens om toegang te krijgen tot systemen en bieden verhoogde, onbeperkte toegang. Beheerders gebruiken deze accounts om besturingssystemen, applicaties en netwerkapparaten te implementeren en te beheren. Deze account moet worden beveiligd of verwijderd om deze risico's

te beperken.

## Administratieve maatregelen (cont.)

### 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 (2<sup>e</sup> en 3<sup>e</sup> bachelor)



### Logboeken en waarschuwingen

- Een logboek registreert **gebeurtenissen** op een systeem
- Bevatten uitgebreide **informatie** voor elke gebeurtenis
- Belangrijk voor computerbeveiliging (AAA: accounting)

**HO  
GENT**

## Administratieve maatregelen (cont.)

### Group Policies

In de meeste netwerken die Windows-computers gebruiken, configureert een beheerder Active Directory met domeinen op een Windows Server. Een beheerder configureert gebruikersaccountbeleid, zoals wachtwoordbeleid en vergrendelingsbeleid door gebruikers aan groepen toe te voegen en beleid op groepsniveau in te stellen.

### Logboeken en waarschuwingen

Een logboek registreert gebeurtenissen zoals ze zich voordoen op een systeem. Logboekvermeldingen vormen een logboekbestand en een logboekvermelding bevat alle informatie met betrekking tot een specifieke gebeurtenis. Logboeken die betrekking hebben op computerbeveiliging zijn steeds belangrijker geworden.

## Fysieke bescherming van een server

### Stroomvoorziening

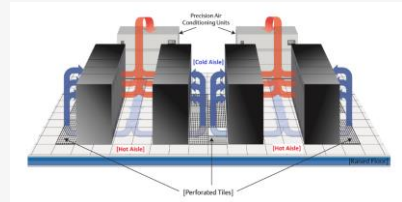
- **Cruciaal** bij beschermen van informatiesystemen
- **Continue levering** noodzakelijk voor server- en gegevensopslagfaciliteiten

### 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



**HO  
GENT**

## Fysieke bescherming van een server

### Stroomvoorziening

Een cruciaal probleem bij het beschermen van informatiesystemen zijn elektrische stroomsystemen en stroomoverwegingen. Een continue levering van elektrische stroom is van cruciaal belang in de huidige enorme server- en gegevensopslagfaciliteiten.

### Verwarming, ventilatie en airconditioning (HVAC)

HVAC-systemen zijn cruciaal voor de veiligheid van mensen en informatiesystemen in de faciliteiten van de organisatie. Bij het ontwerpen van moderne IT-faciliteiten spelen deze systemen een zeer belangrijke rol in de algehele beveiliging. HVAC-systemen regelen de omgevingsomgeving (temperatuur, vochtigheid, luchtstroom en luchtfiltering) en moeten worden gepland en gebruikt samen met andere datacentercomponenten zoals computerhardware, bekabeling, gegevensopslag, brandbeveiliging, fysieke beveiligingssystemen en stroomvoorziening.



## **Hardware monitoring**

Hardware monitoring wordt vaak aangetroffen in grote server farms. Een serverfarm is een faciliteit die honderden of duizenden servers voor bedrijven huisvest.

**7.3**

# **Network Hardening**

**HO  
GENT**

## Netwerkapparaten beschermen

### Network Operations Centers (NOC)

- Op één of meerdere locaties
- Bieden gedetailleerde **status van netwerk**
- Ground zero voor oplossen van netwerkproblemen, prestatiebewaking, software distributie en updates, communicatiebeheer en apparaatbeheer



**HO  
GENT**

## Netwerkapparaten beschermen

### Network Operations Centers

Het Network Operations Center (NOC) bestaat uit één of meerdere locaties met de tools die beheerders een gedetailleerde status van het netwerk van de organisatie bieden. Het NOC is ground zero voor het oplossen van netwerkproblemen, prestatiebewaking, software distributie en updates, communicatiebeheer en apparaatbeheer.

## Netwerkapparaten beschermen (cont.)

### Switches, routers en netwerktoestellen

- **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 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

**HO  
GENT**

## Netwerkapparaten beschermen (cont.)

### Switches, routers en netwerktoestellen

Netwerkapparaten worden geleverd zonder wachtwoorden of standaardwachtwoorden.

- **Netwerkswitches** vormen het hart van het moderne datacommunicatienetwerk. De belangrijkste bedreiging voor netwerkswitches zijn diefstal, hacking en toegang op afstand, aanvallen op netwerkprotocollen zoals ARP / STP of aanvallen op prestaties en beschikbaarheid.
- **VLANs** bieden een manier om apparaten binnen een LAN en op individuele switches te groeperen. VLANs gebruiken logische verbindingen in plaats van fysieke verbindingen.
- **Firewalls** zijn hardware- of softwareoplossingen die netwerkbeveiligingsbeleid afdwingen. Een firewall voorkomt dat ongeautoriseerd of potentieel gevaarlijk verkeer het netwerk binnenkomt.

## Netwerkapparaten beschermen (cont.)

- **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

**HO  
GENT**

## Netwerkapparaten beschermen (cont.)

- **Routers** vormen de ruggengraat van internet en communicatie tussen verschillende netwerken. Routers communiceren met elkaar om het best mogelijke pad te bepalen om verkeer naar verschillende netwerken te sturen. Routers gebruiken routeringsprotocollen om routeringsbeslissingen te nemen.
- **Draadloze en mobiele apparaten** zijn het overheersende type apparaat geworden op de meeste moderne netwerken. Ze bieden mobiliteit en gemak, maar brengen tal van kwetsbaarheden met zich mee. Deze kwetsbaarheden omvatten 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,

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
- **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



**HO  
GENT**

### Spraak- en videoapparatuur

- **VoIP-apparatuur** gebruikt netwerken zoals internet om te bellen en gebeld te worden. De apparatuur die nodig is voor VoIP omvat een internetverbinding en een telefoon.
- **Camera's** - 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, waaronder computersystemen, laptops, tablets en smartphones. Camera's zijn er in verschillende vormen, waaronder de traditionele beveiligingscamera.
- **Videoconferentieapparatuur** maakt het mogelijk dat twee of meer locaties gelijktijdig communiceren met behulp van telecommunicatietechnologieën. Deze technologieën maken gebruik van de nieuwe HD-videostandaarden. Videoconferenties maken nu deel uit van de normale dagelijkse activiteiten in industrieën zoals de medische sector.
- **Netwerk- en IoT-sensoren** - Een van de snelst groeiende sectoren

van informatietechnologie is het gebruik van intelligente apparaten en sensoren. De computerindustrie noemt deze sector het Internet of Things (IoT). Bedrijven en consumenten gebruiken IoT-apparaten om processen te automatiseren, omgevingen te monitoren en de gebruiker te waarschuwen voor ongunstige omstandigheden.



## **7.4**

# **Fysieke beveiliging**

**HO  
GENT**

## 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

**HO  
GENT**

## Fysieke toegangscontrole

### Omheiningen en barricades

Fysieke barrières zijn het eerste dat in je opkomt als je aan fysieke veiligheid denkt. Dit is de buitenste beveiligingslaag en deze oplossingen zijn het meest publiekelijk zichtbaar. Een perimeterbeveiligingssysteem bestaat doorgaans uit een omheiningssysteem, een beveiligingspoortstelsysteem, meerpalen, slagbomen voor het betreden van voertuigen en schuilplaatsen voor bewakers.

### Biometrie

Biometrie zijn de geautomatiseerde methoden om een persoon te herkennen op basis van een fysiologisch of gedragskenmerk.

Biometrische authenticatiesystemen omvatten metingen van het gezicht, vingerafdruk, handgeometrie, iris, netvlies, handtekening en stem. Biometrische technologieën kunnen de basis vormen voor zeer veilige identificatie- en persoonlijke verificatieoplossingen.

## **Badges en toegangslogboeken**

Een badge geeft een persoon toegang tot een gebied met geautomatiseerde toegangspunten. Een toegangspunt kan een deur, een tourniquet, een poort of een andere slagboom zijn. 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 waar toegang heeft verkregen.

## 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**

**HO  
GENT**

## Bewaking

### Bewakers en escorts

Alle fysieke toegangscontroles, inclusief afschrik- en detectiesystemen, zijn uiteindelijk afhankelijk van personeel om in te grijpen en de daadwerkelijke aanval of indringing te stoppen. In sterk beveiligde informatiesysteemfaciliteiten controleren bewakers de toegang tot de gevoelige gebieden van de organisatie.

### Videobewaking en elektronische bewaking

Dit type bewaking kan beveiligingspersoneel aanvullen of in sommige gevallen vervangen. Het voordeel van video- en elektronische bewaking is de mogelijkheid om gebieden te bewaken, zelfs als er geen bewakers of personeel aanwezig zijn, de mogelijkheid om bewakingsvideo's en -gegevens gedurende lange perioden op te nemen en te loggen, en de mogelijkheid om bewegingsdetectie en -melding op te nemen.

## **RFID en draadloze bewaking**

Dit soort bewaking wordt gebruikt om belangrijke informatiesystemen te beheren en te lokaliseren.



Lab oefening:  
**Bescherm je digitale zelf!**