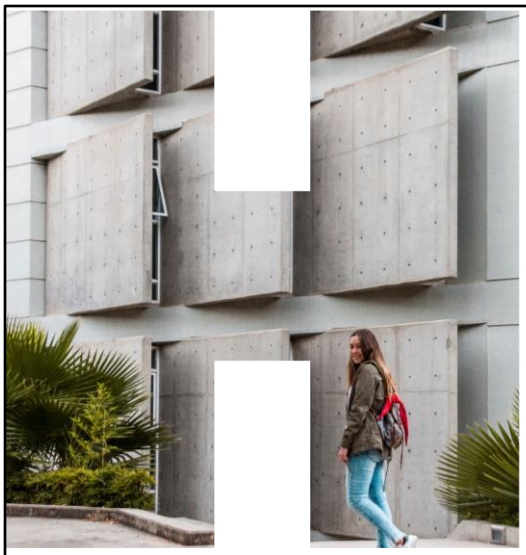

HO
GENT



Cybersecurity

8. Werken als cybersecurity-specialist

HO GENT

8. Werken als cybersecurity-specialist

8.1 De verschillende cybersecurity domeinen
8.2 De ethiek van werk in cybersecurity
8.3 De volgende stap

HO
GENT

8.1 De verschillende cybersecurity domeinen

HO
GENT

Het gebruikersdomein

- **Veel voorkomende bedreigingen en kwetsbaarheden**
  - **Het gebruikersdomein omvat de gebruikers die toegang hebben tot de data van een organisatie**
  - **Bv. werknemers, klanten, onderaannemers, …**
  - **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**

HO GENT

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**

Device Domain Threats	Countermeasure to Manage Threat
Unattended workstations	Establish user account policies for passwords and threshold lockouts
User downloads	Establish access control policies, standards, procedures, and guidelines
Unpatched software	Update and apply security patches according to defined policies, standards, procedures, and guidelines
Malware	Enable an automated antivirus solution to scan systems and update antivirus software
Unauthorized media	Disable internal CD drives and USB ports
Acceptable Use Policy Violation	• Use content filtering • Use antivirus scanning for downloaded files • Disable internal CD drives and USB port

HO GENT

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**

LAN Domain Threats	Countermeasure to Manage Threat
Unauthorized LAN access	• Secure wiring closets, data centers, computer rooms • Define strict access control policies, procedures, and guidelines
Unauthorized access to systems, applications, and data	• Define strict access control policies, procedures, and guidelines • Restrict access privileges for folders and files based on need
Network operating system software vulnerabilities	• Implement policy to patch and update operating systems
Network operating system unpatched	• Implement policy to patch and update operating systems
Unauthorized access by rogue users	• Require passphrases or authentication for wireless networks
Exploits of data in-transit	• Implement encryption between devices and wireless networks
LAN servers with different hardware or operating systems	• Implement LAN server configuration standards
Unauthorized network probing and port scanning	• Conduct post-configuration penetration tests
Firewall misconfiguration	• Conduct post-configuration penetration tests

HO GENT

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**

Private Cloud Domain Threats	Countermeasure to Manage Threat
Unauthorized network probing and port scanning	• Disable ping, probing, and port scanning
Unauthorized access to resources	• Implement intrusion detection and prevention systems
Router, firewall, or network device operating system software vulnerability	• Update devices with security fixes and patches
Router, firewall, or network device configuration error	• Conduct penetration tests post configuration • Test inbound and outbound traffic
Remote users download sensitive data	• Implement data classification standard • Implement file transfer monitoring and scanning

HO GENT

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**

Public Cloud Domain Threats	Countermeasure to Manage Threat
Data breaches	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Loss or theft of intellectual property	• Due diligence • Use of encryption • Data backup
Compromised credentials	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Use of federated identity repositories	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Account hijacking	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Lack of understanding on the part of organization	• Due diligence on agreement responsibilities
Social engineering attacks that lure the victim	• Security awareness programs
Compliance violations	• Due diligence • Policies

HO GENT

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**

Physical Facilities Domain Threats	Countermeasure to Manage Threat
Natural threats including weather and geological problems	• Develop a disaster recovery plan • Develop a business continuity plan
Unauthorized access to facilities	• Implement badge encryption for entry access
Power interruptions	• Develop a disaster recovery plan
Social engineering	• Implement badge encryption for entry access • Conduct security awareness training regularly
Breach of electronic perimeter defenses	• Test building security using both cyber and physical means to covertly gain access
Theft	• Implement an asset tagging system • Establish policies and procedures for visitors
An open lobby	• Implement badge encryption for entry access
Lack of surveillance	• Implement CCTV coverage of all entrances • Test building security using both cyber and physical means to covertly gain access
An unlocked data center	• Implement badge encryption for entry access

HO GENT

Het applicatiedomein

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

Application Domain Threats	Countermeasure to Manage Threat
Unauthorized access to data centers, computer rooms, and wiring closets	• Policies, standards, and procedures for staff and visitors
Server downtime for maintenance	• Disaster recovery plan • Business continuity plan
Network operating system software vulnerability	• Patches and updates completed regularly
Unauthorized access to systems	• Multi-factor authentication • Monitor log files
Data loss	• Data classification standards • Backup procedures
Downtime of IT systems for an extended period	• Disaster recovery plan • Business continuity plan
Software development vulnerabilities	• Conduct software testing prior to launch

HO GENT

8.2 De ethiek van werk in cybersecurity

HO GENT

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 hinken achterop 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)**

HO GENT

Cyberwetten en aansprakelijkheid

- **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, …**


CENTRE FOR
CYBER SECURITY
BELGIUM


HO
GENT

Websites over cybersecurity

- **National Vulnerability Database (NVD)**
- **Computer Emergency Response Team (CERT)**
- **Internet Storm Center (ISC)**
- **The Advanced Cyber Security Center (ACSC)**
- **…**

HO GENT

National Vulnerability Database (NVD): een geautomatiseerde databank van kwetsbaarheden gehost door het NIST.
https://nvd.nist.gov

Computer Emergency Response Team (CERT): helpt overheden en organisaties met het beveiligen van software systemen en netwerken. Ze bestuderen cybersecurity problemen en ontwikkelen methodes en tools om deze tegen te gaan.
https://sei.cmu.edu/about/divisions/cert/
https://cert.be

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.
https://isc.sans.edu/

The Advanced Cyber Security Center (ACSC): een non-profit organisatie dat samenwerkt met overheden, academici en industry

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.
https://www.acscenter.org

Websites over cybersecurity

- **Het is enorm belangrijk om op de hoogte te blijven van de laatste bedreigingen en verdedigingen!**
  - https://www.reddit.com/user/goretsky/m/security (verzameling van reddit threads i.v.m. cybersecurity)
  - https://www.csoonline.com
  - https://www.darkreading.com
  - https://www.bleepingcomputer.com
  - https://news.ycombinator.com
  - https://nakedsecurity.sophos.com
  - https://threatpost.com
  - https://blog.erratasec.com
  - https://krebsonsecurity.com
  - https://medium.com/mitre-attack
  - https://risky.biz
  - https://latesthackingnews.com
  - ...

HO GENT

Cybersecurity wapens

- **Vulnerability scanners**
- **Penetrating testing**
- **Packet analyzers (packet sniffers**
- **Security tools**

HO GENT

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 enloggen 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

HO GENT

8.3 Cybersecurity profielen

Rollen

- **Ook defensie (de militaire inlichtingen dienst, 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.**

HO GENT

Ook defensie (de militaire inlichtingen dienst, ADIV) werft af en toe Cybersecurity specialisten aan. Meer bepaald bij de dienst Cyber Security Operations Centre (CSOC), dat de computernetwerken en wapensystemen van de Belgische krijgsmacht in de gaten houdt en beveiligt tegen cyberaanvallen. Je werkt dan voor het Ministerie van Defensie – Militaire Inlichtingen- en Veiligheidsdienst – Directie Cyber.

Als lid van de militaire cybercapaciteit sta je in voor het beschermen van de militaire informatie en het garanderen van de integriteit en de beschikbaarheid van de militaire netwerken en wapensystemen. Als enige overheidsdienst heeft de militaire inlichtingen- en veiligheidsdienst het wettelijk mandaat gekregen om, naast klassieke defensieve cybercapaciteiten, ook cyberexpertise te ontwikkelen voor het verwerven van inlichtingen en voor het ondersteunen en uitvoeren van militaire operaties.

De opdrachten worden anders ingevuld naargelang je specifieke rol.

8.3 Cybersecurity profielen

Rollen

- **Als Vulnerability Assessor, neem je deel aan het risicobeoordelingsproces van de interne en externe IT-omgevingen.**
- **Als Threat Analyst identificeer, verzamel en analyseer je de informatie over dreigingen tegen het netwerk.**
- **Als Incident Handler ga je op zoek naar mogelijke aanvallen, door het doorzoeken van de beschikbare logs en van allerhande veiligheidsmeldingen.**
- **Als Digital Forensics Analyst spits je je volledig toe op het onderzoek van images van geheugen of harde schijven.**
- **Als Malware Analyst voer je gedetailleerde analyses uit van malware.**

HO GENT

Als **Vulnerability Assessor** neem je deel aan het risicobeoordelingsproces van de interne en externe IT-omgevingen door het uitvoeren van een vulnerability assessment, een security assessment van de softwareproducten gebruikt door de organisatie, een technische audit van de informatiesystemen en indien nodig penetratietesten. Je evalueert en rapporteert aan het management de beveiligingsmaatregelen en de naleving van de regels, normen en het beleid van de organisatie. Je bestudeert nieuwe technologieën om vulnerabilities te identificeren en om de preventieve maatregelen te implementeren.

Als **Threat Analyst** identificeer, verzamel en analyseer je de informatie over dreigingen tegen netwerk- en wapensystemen van Defensie. Dit doe je op een proactieve wijze om de detectie van cyberaanvallen tegen deze systemen te kunnen verbeteren. Je bent verantwoordelijk voor het vormen van een zo duidelijk mogelijk beeld van de cyberdreiging. Je doet dit door de capaciteiten en de intenties van mogelijke tegenstanders in kaart te brengen. Je documenteert tevens de grote malware families op basis van

informatie die je verzamelt afkomstig van publieke bronnen (van bijvoorbeeld antivirus bedrijven) als uit gesloten bronnen (van bijvoorbeeld eigen detectie en bevriende inlichtingendiensten). Je houdt systematisch relevante Indicators of Compromise (IoCs) bij. Je zorgt ervoor dat deze correct beschikbaar zijn op de detectiesystemen van de beschermde netwerken.

Als **Incident Handler** ga je op zoek naar mogelijke aanvallen, door het doorzoeken van de beschikbare logs en van allerhande veiligheidsmeldingen. Bij een reële cyberaanval isoleer je en verwijder je de gevonden infecties. De betrokken bestanden geef je door voor verdere analyse. Je zet een aangepast detectienetwerk op en je onderhoudt de detectiemiddelen en -regels. Je stuurt dit systeem permanent bij volgens de evolutie van de dreiging.

Als **Digital Forensics Analyst** spits je je volledig toe op het onderzoek van images van geheugen of harde schijven om je werk te doen. Dit kunnen images zijn van alle mogelijke toestellen die voor Defensie van belang zijn. Het doel is ofwel om samples van infecties te kunnen detecteren, ofwel om specifieke gebruiksfeiten van deze toestellen op te sporen.

Als **Malware Analyst** voer je gedetailleerde analyses uit van malware. Je doet dit met behulp van specifieke tools. Je bepaalt mee de Indicators of Compromise (IoC's) om de detectie te ondersteunen. Je schrijft op maat gemaakte detectie- of desinfectietools waarbij je je baseert op de resultaten van je eigen analyses of deze van je collega's. Dit moet een betere verdediging mogelijk maken tegen malware die in commerciele tools niet gekend zijn.

8.4 De volgende stap

HO
GENT

Verken de inhoud van het werk van een cybersecurity specialist

- **Het ISO cybersecurity 27000 model vermelt 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**

HO GENT

Verken de inhoud van het werk van een cybersecurity specialist

- Er zijn verschillende websites waar je kan zoeken naar vacatures in cybersecurity nadat je afstudeert
  - https://vdab.be/vindeenjob/jobs/cyber-security-consultant
  - https://be.indeed.com/Cyber-Security-jobs
  - https://ictjob.be/nl/it-vacatures-zoeken/cyber-security
  - https://be.linkedin.com/jobs/cyber-security-jobs

HO GENT


HO
GENT