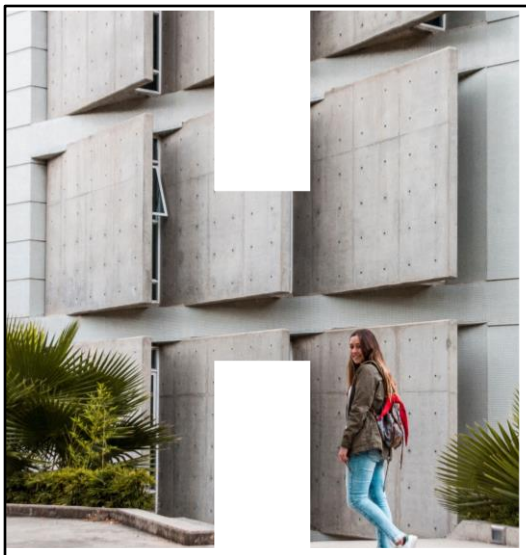

HO
GENT



NEW

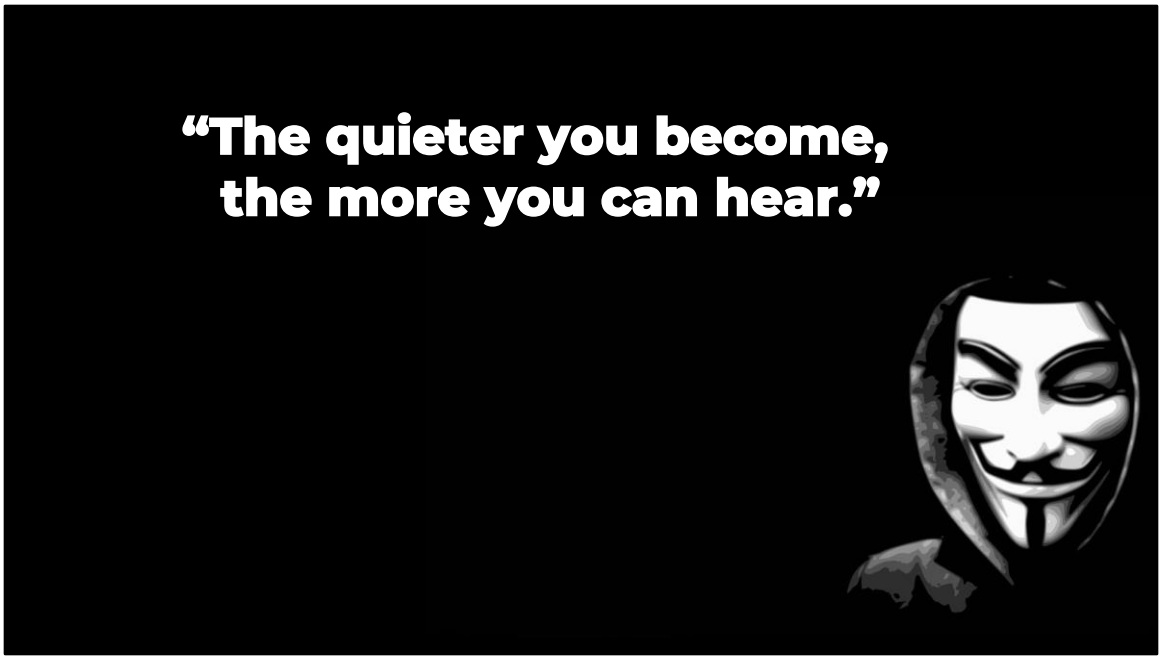
Cybersecurity

2020-2021

1. Een wereld van experten en criminelen

cisco HO GENT

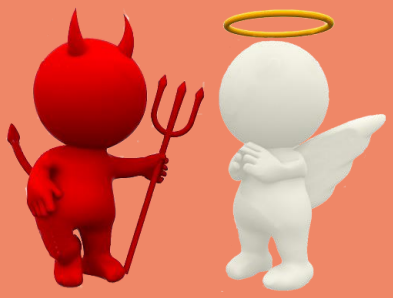
Een opwarmer … de link met cybersecurity lijkt misschien vaag, maar de vraag op het einde zou je ook kunnen formuleren als "Wie is de beste hacker?". Stel dat je netwerkverkeer wil sniffen in een bedrijfsnetwerk en je plaatst hiervoor een rogue apparaat dat verbonden is met een (netwerk)printer. Als jouw rogue apparaat gaat schreeuwen dat hij in het netwerk zit, zal het apparaat snel ontdekt worden en de aanval mislukken. Als je apparaat echter zo goed als onzichtbaar is …



Wie ooit Kali Linux installeert (een Linux distributie met veel vooraf geïnstalleerde cybersecurity tools, populair bij hackers en cybersecurity experten), zal merken dat deze boodschap terugkomt in veel van de ingebouwde wallpapers. Een goede hacker is immers stil en onzichtbaar, en wacht geduldig af tot het juiste moment om toe te slaan.

1. Een wereld van experten en criminelen

1.1 De wereld van cybersecurity
1.2 Criminelen vs. specialisten
1.3 Typische cyberaanvallen
1.4 Verspreiding van cyberaanvallen
1.5 Nood aan experten
1.6 Samenvatting



HO
GENT

1.1
De wereld van cybersecurity

HO
GENT

Websites en de kracht van data

- Innovatieve bedrijven zoals Facebook zijn ontstaan door de kracht van data en data-analyse te verzamelen en te benutten.
- Deze bedrijven hebben de verantwoordelijkheid om deze gegevens te beschermen tegen misbruik en ongeoorloofde toegang.
- De groei van data heeft geweldige kansen gecreëerd voor cybersecurity-specialisten.

HO GENT

Domeinen

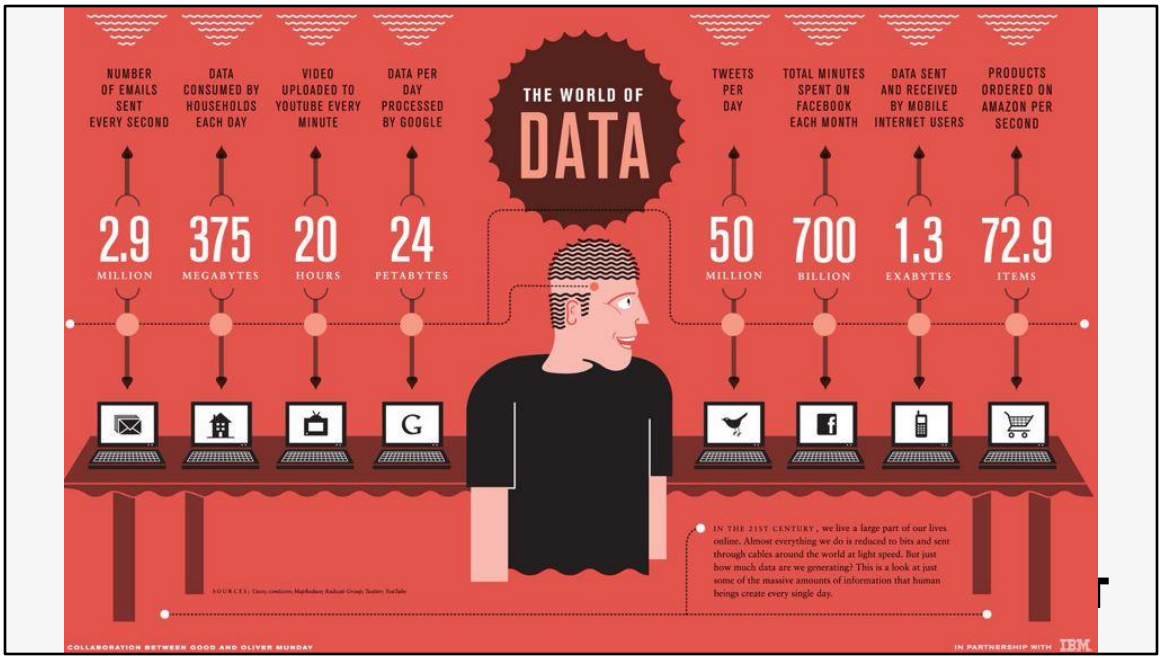
- Grote en kleine bedrijven hebben de kracht van big data en data-analyse ingezien.
- Organisaties zoals Google, LinkedIn en Amazon bieden belangrijke diensten en kansen voor hun klanten.
- De groei in gegevensverzameling en -analyse brengt grote risico's met zich mee voor individuen en het moderne leven als er geen voorzorgsmaatregelen worden genomen om gevoelige gegevens te beschermen tegen criminelen of anderen die van plan zijn schade te berokkenen.

HO GENT

Groeiende verzameling data

- Cyberexperten hebben nu de technologie om wereldwijd weertrends te volgen, de oceanen te volgen en de bewegingen en het gedrag van mensen, dieren en objecten in real time te volgen.
- Nieuwe technologieën, zoals Geospatial Information Systems (GIS) en het Internet of Everything (IoE), zijn in opkomst. Deze technologieën zijn gebaseerd op het verzamelen en analyseren van enorme hoeveelheden gegevens.
- Deze groeiende verzameling gegevens kan mensen helpen energie te besparen, de efficiëntie te verbeteren en veiligheidsrisico's te verminderen.

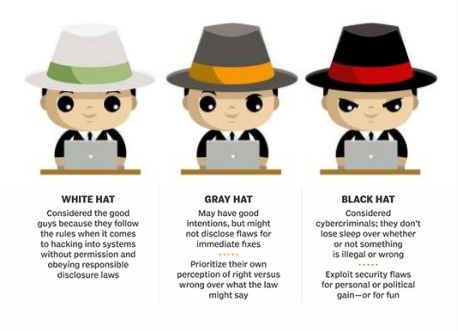
HO GENT


THE WORLD OF
DATA
NUMBER OF EMAILS SENT EVERY SECOND
2.9 MILLION
DATA CONSUMED BY HOUSEHOLDS EACH DAY
375 MEGABYTES
VIDEO UPLOADED TO YOUTUBE EVERY MINUTE
20 HOURS
DATA PER DAY PROCESSED BY GOOGLE
24 PETABYTES
TWEETS PER DAY
50 MILLION
TOTAL MINUTES SPENT ON FACEBOOK EACH MONTH
700 BILLION
DATA SENT AND RECEIVED BY MOBILE INTERNET USERS
1.3 EXABYTES
PRODUCTS ORDERED ON AMAZON PER SECOND
72.9 ITEMS
IN THE 21ST CENTURY, we live a large part of our lives online. Almost everything we do is reduced to bits and sent through cables around the world at light speed. But just how much data are we generating? This is a look at just some of the massive amounts of information that human beings create every single day.
COLLABORATION BETWEEN GOOD AND OLIVER MUNDAY
IN PARTNERSHIP WITH IBM

1.2 Criminelen vs. specialisten

HO GENT

Hackers



Een hacker (aanvaller) kan om verschillende redenen inbreken op computers of netwerken om toegang te verkrijgen:

- White hat hackers breken in op netwerken of computersystemen om zwakke punten te ontdekken en zo de beveiliging van deze systemen te verbeteren.
- Gray hat hackers bevinden zich ergens tussen de 2 andere types aanvallers. Deze aanvallers kunnen een kwetsbaarheid vinden en deze melden aan de eigenaren van het systeem als die actie samenvalt met hun agenda.
- Black hat hackers zijn onethische criminelen die de computer- en netwerkbeveiliging schenden voor persoonlijk gewin of om kwaadaardige redenen, zoals het aanvallen van netwerken.

HO GENT

Cybercriminelen

Criminelen zijn er in veel verschillende vormen. Elk heeft zijn eigen motieven:

- Script Kiddies
  Dit zijn meestal tieners of hobbyisten, en hun aanvallen zijn meestal beperkt tot grappen en vandalisme. Ze hebben weinig of geen vaardigheid en gebruiken vaak bestaande tools of instructies op internet om aanvallen uit te voeren.
- Vulnerability Brokers (NL: Kwetsbaarheidsbemiddelaars)
  Dit zijn 'gray hat' aanvallers die exploits proberen te ontdekken en deze aan leveranciers rapporteren, soms voor geldprijzen of beloningen.
- Hacktivisten
  Dit zijn 'gray hat' aanvallers die zich verzamelen en protesteren tegen verschillende politieke en sociale ideeën. Hacktivisten protesteren publiekelijk tegen organisaties of regeringen door artikelen en video's te plaatsen, gevoelige informatie te lekken en DDoS-aanvallen (Distributed Denial of Service) uit te voeren.

HO GENT

Cybercriminelen (cont.)

- Cybercriminelen
  Black hat hackers die ofwel als zelfstandige werken of voor grote cybercrime-organisaties werken. Elk jaar zijn cybercriminelen verantwoordelijk voor het stelen van miljarden dollars van consumenten en bedrijven.
- Door de staat gesponsorde hackers
  Afhankelijk van het perspectief van een persoon, zijn dit ofwel white hat ofwel black hat hackers die overheidsgeheimen stelen, inlichtingen verzamelen en netwerken saboteren. Hun doelwitten zijn buitenlandse regeringen, terroristische groeperingen en bedrijven. De meeste landen in de wereld nemen tot op zekere hoogte deel aan door de staat gesponsorde hacking.

HO GENT

1.2 – Criminelen vs. specialisten

Cybersecurity Specialisten

Het dwarsbomen van de cybercriminelen is een moeilijke taak. Vele bedrijven, de overheden en internationale organisaties zijn daarom begonnen met het nemen van gecoördineerde acties om cybercriminelen te beperken of af te weren. Deze omvatten:

- Vulnerability Databases
  Publiek beschikbare databases van gekende kwetsbaarheden
- Early Warning Systems
  Systemen voor vroegtijdige waarschuwing
- Share Cyber Intelligence
  Delen van cyber intelligence, vaak door middel van samenwerking tussen de publieke en private sector.
- ISM normen (bv. ISO 27000)
  Standaarden en normen voor informatiebeveiligingsbeheer die een kader vormen voor het implementeren van beveiligingsmaatregelen binnen een organisatie.

HO GENT

Vulnerability Databases (kwetsbaarheidsdatabases):
De Nation Common Vulnerabilities and Exposures (CVE) -database is een voorbeeld van de ontwikkeling van een nationale database in de VS. Het doel van de CVE National Database is om een publiek beschikbare database aan te bieden met alle bekende kwetsbaarheden (zie http://www.cvedetails.com).

Early Warning Systems:
Het Honeynet-project is een voorbeeld van van een system voor vroegtijdige waarschuwing. Het project biedt een HoneyMap die een real-time visualisatie van aanvallen weergeeft (zie https://www.honeynet.org/node/960).

Share Cyber Intelligence:
InfraGard is een voorbeeld van het wijdverbreid delen van cyber intelligence. Het InfraGard-programma is een samenwerkingsverband tussen de en de private sector. De deelnemers zijn toegewijd aan het delen van informatie en intelligentie om vijandige cyberaanvallen te voorkomen (zie

https://www.infragard.org/).

ISM Normen:
De ISO 27000-normen zijn een voorbeeld van normen voor informatiebeveiligingsbeheer. De standaarden bieden een kader voor het implementeren van cyberbeveiligingsmaatregelen binnen een organisatie (zie http://www.27000.org/).

Een beeld uit een Anonymous-video uit 2016. De presentator, met het iconische Guy Fawkes-masker, kondigt een operatie aan tegen IS.

Complottheorieën over corona, 5G en aliens: is hackerscollectief Anonymous nu zelf gehackt?

In de nasleep van #BlackLivesMatter hebben hackers onder de naam Anonymous Amerikaanse politiewebsites platgelegd. Heel even leek het weer vier jaar geleden, de hoogdagen van de beweging. Maar toch klinkt Anonymous anno 2020 anders dan vroeger. Waanzinniger. De internetbeweging gaat nu immers ook tekeer tegen 5G, Bill Gates en zelfs buitenaardse wezens die de wereld zouden besturen.

wo 12 aug @ 17:38

https://vrtnws.be/p.43d39eq65

HO GENT

1.3 Typische cyberaanvallen

HO GENT

Bedreigingen en kwetsbaarheden

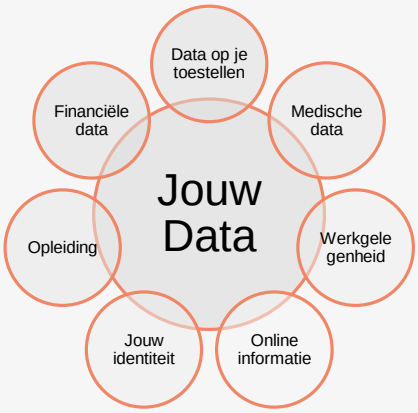
- Cybersecurity-specialisten hebben het inzicht om de invloed van data te erkennen en die kracht te gebruiken om geweldige organisaties op te bouwen, diensten te verlenen en mensen te beschermen tegen cyberaanvallen
- Cybersecurity-specialisten erkennen de dreiging die gegevens vormen als ze tegen mensen worden gebruikt
- Een cyberbeveiligingsdreiging (*en:* cybersecurity threat) is de mogelijkheid dat zich een schadelijke gebeurtenis, zoals een aanval, voordoet
- Cyberkwetsbaarheid (*en:* cyber vulnerability) is een zwakte die een doelwit vatbaar maakt voor een aanval
- Cyberdreigingen zijn bijzonder gevaarlijk voor bepaalde bedrijfstakken en voor het soort informatie dat ze verzamelen en beschermen

HO GENT

Bedreiging Arena's

Enkele voorbeelden van "interessante" data die afkomstig kunnen zijn van gevestigde organisaties:

- Persoonlijke informatie
- Medische gegevens
- Onderwijsgegevens
- Werkgelegenheid en financiële gegevens



HO GENT

Doelwitten

Netwerkdiensten zoals DNS, HTTP en online databases zijn de belangrijkste doelwitten voor cybercriminelen.

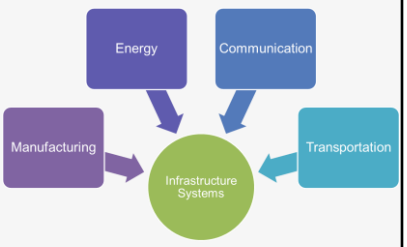
- Criminelen gebruiken vaak specifieke sniffing tools die alle verkeer over een netwerk opneemt en bewaart.
- Criminelen kunnen ook frauduleuze (rogue) apparaten gebruiken, zoals onbeveiligde Wi-Fi-toegangspunten.
- Vaak worden valse berichten verspreid binnen een netwerk. De berichten worden zo opgesteld dat het lijkt alsof ze deel uitmaken van echte communicatie.

HO GENT

1.3 – Typische cyberaanvallen

Meer dan persoonlijke data

- Hackers zijn niet enkel geïnteresseerd in jouw persoonlijke data maar richten zich ook vaak tot netwerken van de industrie
  - Vaak met als doel om losgeld te vragen
- In bedrijven is niet alles home equipment, doelwitten zijn vaak meer dan enkel computers
  - Bv. SCADA (Supervisory Control And Data Acquisition) voor de meting en sturing van verschillende machines in grote industriële systemen.



HO GENT

Typische domeinen zijn onder meer:

- Productie
  - Branchecontroles
  - Automatisering
  - SCADA
- Energieproductie en –distributie
  - Elektrische distributie en Smart Grid
  - Olie en gas
- Communicatie
  - Telefoon
  - E-mail
  - Berichten
- Transportsystemen
  - Vliegreizen
  - Het spoor
  - Op de weg

Hoe beschermen?

- Op persoonlijk vlak moet iedereen zijn of haar identiteit, gegevens en computerapparatuur beschermen.
- Op bedrijfsniveau is het de verantwoordelijkheid van de medewerkers om de reputatie, gegevens en klanten van de organisatie te beschermen.
- Op staatsniveau staan de nationale veiligheid en de veiligheid en het welzijn van de burgers op het spel.
  - In de VS is de National Security Agency (NSA) verantwoordelijk voor het verzamelen van inlichtingen en bewakingsactiviteiten.
- De inspanningen om de manier van leven van mensen te beschermen, zijn vaak in strijd met hun recht op privacy.
  - Zie ook de hele problematiek rond de Belgische “contact tracing app”

HO GENT

1.4

Verspreiding van ~~covid~~ cyberaanvallen

Interne vs. externe aanvallen

Aanvallen kunnen afkomstig zijn van binnen een organisatie of van buiten de organisatie

Interne aanvallen

- Afkomstig van een interne gebruiker, zoals een medewerker of contractpartner. Kan per ongeluk of opzettelijk zijn.
- Interne aanvallen kunnen grotere schade aanrichten dan externe dreigingen, omdat interne gebruikers rechtstreeks toegang hebben tot het gebouw en de bijbehorende infrastructuur/apparatuur.
- Interne aanvallers hebben doorgaans kennis van het bedrijfsnetwerk, de bronnen en de vertrouwelijke gegevens. Ze hebben mogelijk ook kennis van beveiligingsmaatregelen, beleidsregels en hogere niveaus van beheerdersrechten.

Externe aanvallen

- Externe aanvallen van amateurs of ervaren aanvallers kunnen misbruik maken van kwetsbaarheden in netwerkapparaten, of kunnen social engineering gebruiken, zoals bedrog, om toegang te krijgen.
- Externe aanvallen maken misbruik van zwakheden of kwetsbaarheden om toegang te krijgen tot interne bronnen.

HO GENT

Opkomst van mobiele apparaten

- In het verleden gebruikten werknemers doorgaans door het bedrijf uitgegeven computers die waren verbonden met een bedrijfsnetwerk.
- Tegenwoordig worden mobiele apparaten zoals iPhones, smartphones, tablets en duizenden andere apparaten krachtige vervangers van of toevoegingen aan de traditionele pc.
- Steeds meer mensen gebruiken deze apparaten om toegang te krijgen tot bedrijfsinformatie. Bring Your Own Device (BYOD) is een groeiende trend.
- Het onvermogen om mobiele apparaten centraal te beheren en bij te werken, vormt een groeiende bedreiging voor organisaties die mobiele apparaten van werknemers op hun netwerken toestaan.

HO GENT

Opkomst van Internet-of-Things

- Het Internet of Things (IoT) is de verzameling technologieën die de verbinding van verschillende apparaten met het internet mogelijk maakt.
- IoT-technologieën stellen mensen in staat miljarden apparaten met internet te verbinden. Deze apparaten omvatten lichten, sloten, motoren en entertainmentapparaten, om er maar een paar te noemen.
- Deze technologie heeft invloed op de hoeveelheid gegevens die moet worden beschermd. Gebruikers hebben op afstand toegang tot deze apparaten, waardoor het aantal netwerken dat moet worden beschermd toeneemt.
- Met de opkomst van IoT moeten er veel meer gegevens worden beheerd en beveiligd. Al deze verbindingen, plus de uitgebreide opslagcapaciteit en opslagdiensten die worden aangeboden via de cloud en virtualisatie, hebben geleid tot de exponentiële groei van gegevens.

Impact van Big Data

Big data is het resultaat van datasets die groot en complex zijn, waardoor traditionele dataverwerkingstoepassingen ontoereikend zijn. Big data biedt zowel uitdagingen als kansen op basis van drie dimensies:

- Het volume of de hoeveelheid gegevens
- De snelheid van gegevens
- De verscheidenheid of het bereik van gegevenstypen en bronnen

Er zijn talloze voorbeelden van grote bedrijfshacks in het nieuws. Als gevolg hiervan vereisen bedrijfssystemen ingrijpende veranderingen in het ontwerp van beveiligingsproducten en substantiële upgrades van technologieën en praktijken. Bovendien introduceren overheden en industrieën meer voorschriften en mandaten die betere gegevensbescherming en beveiligingscontroles vereisen om big data te beschermen.

Geavanceerde wapens

- Advanced Persistent Threat (APT) is een voortdurende computerhack die onder de radar plaatsvindt tegen een specifiek object. Criminelen kiezen meestal voor een APT vanwege zakelijke of politieke motieven.
- Algoritme-aanvallen kunnen zelfrapportagegegevens van het systeem volgen, zoals het energieverbruik van een computer, en die informatie gebruiken om doelen te selecteren of valse waarschuwingen te activeren. Algoritmische aanvallen zijn sluwer omdat ze gebruikmaken van ontwerpen die worden gebruikt om energiebesparingen te verbeteren, systeemstoringen te verminderen en de efficiëntie te verbeteren.
- Intelligente selectie van slachtoffers: in het verleden zouden aanvallen het laaghangende fruit of de meest kwetsbare slachtoffers selecteren. Veel van de meest geavanceerde aanvallen worden alleen gestart als de aanvaller de handtekeningen van het beoogde slachtoffer kan evenaren.

HO GENT

1.4 – Verspreiding van cyberaanvallen

Bredere reikwijdte en cascade-effect

- Federatief identiteitsbeheer verwijst naar meerdere ondernemingen die hun gebruikers dezelfde identificatiegegevens laten gebruiken om toegang te krijgen tot de netwerken van alle ondernemingen in de groep. Het doel van federatief identiteitsbeheer is om identiteitsinformatie automatisch over kasteelgrenzen heen te delen.
- De meest gebruikelijke manier om de federatieve identiteit te beschermen, is door inlogmogelijkheid te koppelen aan een geautoriseerd apparaat.

HO GENT

Voorbeelden van federatief identiteitsbeheer:

- Je kan je op verschillende sites inloggen met een facebook- / google- / steam- / … account, ook al heeft die website niets met facebook / google / steam / … te maken
- Je kan je op verschillende sites inloggen met je e-id (elektronische identiteitskaart)

Gevolgen voor de veiligheid

- Er zijn veel veiligheidsimplicaties verbonden aan de duistere krachten van cyberveiligheid, waaronder alarmcentrales in de VS die kwetsbaar zijn voor cyberaanvallen die 911-netwerken zouden kunnen afsluiten, waardoor de openbare veiligheid in gevaar komt.
- Een telefonische denial of service (TDoS) -aanval maakt gebruik van telefoongesprekken tegen een doeltelefoonnetwerk dat het systeem vasthoudt en verhindert dat legitieme oproepen binnenkomen.
- De volgende generatie 911-callcenters zijn kwetsbaar omdat ze Voice-over-IP (VoIP) -systemen gebruiken in plaats van traditionele vaste lijnen.

HO GENT

Verhoogde waakzaamheid

- De verdediging tegen cyberaanvallen aan het begin van het cybertijdperk was laag. Een slimme middelbare scholier of scriptkiddie kon toegang krijgen tot systemen.
- Nu zijn landen over de hele wereld zich meer bewust geworden van de dreiging van cyberaanvallen. De dreiging van cyberaanvallen staat nu in de meeste landen bovenaan de lijst van grootste bedreigingen voor de nationale en economische veiligheid.
  - Hoe doen we het in België?

HO GENT

Indien je slachtoffer of getuige bent van cybercriminaliteit kan je steeds terecht bij de politie:

- Op https://www.safeonweb.be/nl/nuttige-links vind je links voor verschillende soort cybercriminaliteit:
- Je kan steeds aangifte doen bij jouw lokale politie

Wil je controleren of je zelf al eens het slachtoffer bent geweest van een aanval? Surf dan naar https://haveibeenpwned.com/ . Let wel op! Het is niet omdat deze site zegt dat jouw gegevens nog niet zijn teruggevonden online, dat je niet het slachtoffer bent geworden van een aanval. Dat is immers onmogelijk te achterhalen. Deze website heeft enkel weet van aanvallen die publiek ontdekt zijn.

1.5
Nood aan experten

HO
GENT

NIST Framework

- In de VS heeft het National Institute of Standards and Technologies (NIST) een raamwerk gecreëerd voor bedrijven en organisaties die cyberbeveiligingsprofessionals nodig hebben. Het raamwerk stelt bedrijven in staat de belangrijkste soorten verantwoordelijkheden, functietitels en benodigde personeelsvaardigheden te identificeren.
- Het Workforce Framework deelt cybersecuritywerk in zeven categorieën in, deze worden besproken op de volgende slides.

HO GENT

De 7 categorieën van cybersecurity werk

- Operate and Maintain omvat het bieden van de 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 voor interne systemen en netwerken.
- Investigate omvat het onderzoek naar cybergebeurtenissen en / of cybercriminaliteit waarbij IT-middelen zijn betrokken.
- Collect and Operate omvat gespecialiseerde ontkennings- en misleidingsoperaties en het verzamelen van cyberbeveiligingsinformatie.
- Analyze omvat zeer gespecialiseerde beoordeling en evaluatie van inkomende cyberbeveiligingsinformatie om te bepalen of deze nuttig is voor inlichtingen.

HO GENT

De 7 categorieën (cont.)

- Oversight and Development voorziet in leiderschap, management en richting om cyberveiligheid effectief uit te voeren.
- Securely Provision omvat het conceptualiseren, ontwerpen en bouwen van veilige IT-systemen.

Binnen elke categorie zijn er verschillende vakgebieden. De speciale gebieden definiëren vervolgens veelvoorkomende soorten cyberbeveiligingswerk.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

HO GENT

Professionele organisaties

- Cybersecurity-specialisten moeten regelmatig samenwerken met professionele collega's. Internationale technologieorganisaties sponsoren vaak workshops en conferenties.

GENT

Studentenorganisaties en competities

- Cybersecurity-specialisten moeten dezelfde vaardigheden hebben als hackers, vooral black hat-hackers, om zich te beschermen tegen aanvallen.
- Hoe kan een individu de vaardigheden opbouwen en oefenen die nodig zijn om een cyberbeveiligingsspecialist te worden?
- Competities voor studenten zijn een geweldige manier om kennis en vaardigheden op het gebied van cyberbeveiliging op te bouwen.
- In de VS zijn er veel competities voor cybersecurityvaardigheden beschikbaar voor studenten.

HO
GENT

Certificeringen

In een wereld van cyberdreigingen is er een grote behoefte aan bekwame en deskundige informatiebeveiligingsprofessionals. De IT-industrie heeft standaarden opgesteld voor cybersecurity-specialisten om professionele certificeringen te verkrijgen die het bewijs leveren van vaardigheden en kennisniveau.

- CompTIA Security + is een door CompTIA gesponsord testprogramma dat de competentie van IT-beheerders op het gebied van informatieborging certificeert.
- EC-Council Certified Ethical Hacker (CEH) is een certificering op gemiddeld niveau die beweert dat cybersecurity-specialisten met deze referentie over de vaardigheden en kennis beschikken voor verschillende hackpraktijken.
- SANS GIAC Security Essentials (GSEC) is een goede keuze als instapmodel voor cybersecurity-specialisten die kunnen aantonen dat ze de beveiligingsterminologie en -concepten begrijpen en over de vaardigheden en expertise beschikken die nodig zijn voor 'hands-on' beveiligingsrollen. Het SANS GIAC-programma biedt een aantal aanvullende certificeringen op het gebied van beveiligingsadministratie, forensisch onderzoek en auditing.

HO GENT

Certificeringen (cont.)

- (ISC)^2 Certified Information Systems Security Professional (CISSP) is een leverancierneutrale certificering voor die cybersecurity-specialisten met veel technische en managementervaring. Het is ook formeel goedgekeurd door het Amerikaanse ministerie van Defensie (DoD) en is een wereldwijd erkende branchecertificering op het gebied van beveiliging.
- ISACA Certified Information Security Manager (CISM) Cybersecurity-specialisten die verantwoordelijk zijn voor het beheren, ontwikkelen en toezicht houden op informatiebeveiligingssystemen op bedrijfsniveau of voor degenen die de beste beveiligingspraktijken ontwikkelen, kunnen in aanmerking komen voor CISM.
- Cisco Certified Network Associate Security (CCNA Security) valideert dat een cyberbeveiligingsspecialist over de kennis en vaardigheden beschikt die nodig zijn om Cisco-netwerken te beveiligen.

HO GENT

1.5 – Nood aan experten

Hoe word je een cybersecurity expert?

Cybersecurity-specialisten moeten kunnen reageren op dreigingen zodra ze zich voordoen. Dit betekent dat de werktijden wat onconventioneel kunnen zijn. Cybersecurity-specialisten analyseren ook beleid, trends en intelligentie om te begrijpen hoe cybercriminelen denken. Vaak kan dit veel speurwerk met zich meebrengen. Hier is een goed advies om een cybersecurity-specialist te worden:

- Studeer: leer de basis door IT cursussen te volgen. Wees een levenslange leerling. Cybersecurity is een vak dat voortdurend verandert, en cybersecurity-specialisten moeten bijblijven.
- Behaal certificeringen: certificeringen van organisaties zoals Microsoft en Cisco bewijzen dat je over de kennis beschikt die nodig is om werk te zoeken als cybersecurity-specialist.
- Stages: Het zoeken naar een stage binnen het gebied van cybersecurity kan leiden tot opportuniteiten in de toekomst.
- Professionele organisaties: word lid van computerbeveiligingsorganisaties, woon vergaderingen en conferenties bij en sluit u aan bij forums en blogs om kennis op te doen van andere experten.

HO GENT

Een bekende conferentie over cybersecurity en hacking in België is https://brucon.org . Door middel van presentaties, workshops, … blijf je op de hoogte van de laatste en nieuwste cybersecurity weetjes en tools.


HO
GENT