10 CYBERSECURITY

10.1 INLEIDING

- **Cybersecurity:** is het geheel van technologieën, processen en praktijken die zijn ontworpen om netwerken, computers, programma's en gegevens tegen aanval, schade of onbevoegde toegang te beschermen
- **Beveiliging:** In een computercontext omvat beveiliging zowel cybersecurity als fysieke beveiliging

- **Het beveiligen van cybersecurity vereist gecoördineerde inspanningen door middel van een informatiesysteem. Elementen van cybersecurity omvatten:**

  -> applicatiebeveiliging

  -> informatiebeveiliging

  -> netwerk veiligheid

  -> rampherstel / bedrijfscontinuïteit planning

  -> operationele beveiliging

  -> eindgebruikersopleiding

- **Problematische elementen van cybersecurity:**

  -> de snel en voortdurend veranderende aard van beveiligingsrisico's

  -> de traditionele aanpak is om de meeste bronnen op de meest cruciale systeemcomponenten te concentreren en te beschermen tegen de meest bekende dreigingen, waardoor een aantal minder belangrijke systeemcomponenten onbeschermd en wat minder gevaarlijke risico's zijn die niet worden beschermd.

    -> een dergelijke aanpak is onvoldoende in de huidige omgeving

    -> teneinde om te kunnen gaan met de huidige omgeving stimuleren adviesorganisaties een meer proactieve en adaptieve aanpak

- **Cybersecurity (digitale veiligheid) is echter lastig te realiseren op het internet:**

1. Het internet is niet ontworpen om op een veilige manier gebruikt te worden
2. Misbruik is nooit onmogelijk, juist door de wereldwijde toegang tot het internet is de groep potentiële daders veel groter dan in real-life
3. Bij de ontwikkeling van technologie is een veilig systeem niet het uuitgangspnt (het moet eerst werken, aan het eind kijken we naar veiligheid)
4. De mens is de zwakste schakel

- **Incindenten:**

  -> **DigiNotar:**

    -> certificatenleverancier waar in 2011 sccesvol werd ingebroken

    -> er werden op een frauduleuze manier certificaten aangemaakt

    -> hierdoor konden inloggegevens en ander dataverkeer afgetapt worden

    -> escaleerde tot de eerste digitale crisis

    -> belgische en nederlandse overheid zegde het vertrouwen in DigiNotar op

  -> **Patiëntgegevens:**

    -> bij de invoering van EPD's (elektronische patiëntendossiers) bleek veel mis te zijn met de bescherming van de patiëntgegevens

    -> experts konden makkelijk 1.2 miljoen patiëntgegevens bemachtigen en veranderen

  -> **DDoS-aanvallen op banken:**

    -> er vonden veel verschillende aanvallen achter elkaar plaats en de aanval had een lange duur

    -> consumenten ondervonden groot ongemak en bedrijven veel schade

    -> er kon niet met Ideal / pinpassen betaald worden

10.2 WAT IS CYBERSECURITY

- **Hathaway & Klimburg:**

    -> de term cybersecurity is gerelateerd aan de term informatiebeveiliging

- **Nationale cybersecuritystrategie:**

    -> cybersecurity is het vrij zijn van gevaar of schade veroorzaakt door storing of uitval van ICT of door misbruik van ICT

- **Gevaar of de schade door misbruik:**

    -> gevaar of schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie

- **CIA-principe:**

  -> Confidentiality (vertrouwelijkheid), Integrity (integriteit) en Availability (beschikbaarheid).

  -> Soms worden Reliability (betrouwbaarheid) en Authenticity (authenticiteit) toegevoegd (denk aan CIARA)

- **Van Solms & Niekerk:**

  -> cybersecurity is breder dan informatiebeveiliging (denk o.a. ook aan cyberterrorism en digitale media)

  -> veiligheid op internet kan ook onveilige situaties omvatten die niet door beveiliging zijn op te lossen.

  -> ook het omgekeerde is echter waar: soms is informatiebeveiliging breder dan cybersecurity

- **ICT verwijst niet alleen naar het internet:**

  -> ICT staat voor alle informatie- en communicatietechnologieën.

  -> de term informatiebeveiliging in combinatie met ICT ligt meer voor de hand

- **Cybersecurity:**

  -> nadruk ligt op beveiligen en weerbaarder maken van systemen en netwerken

  -> hierbij moet inzicht verkregen worden in potentiële kwetsbaarheden, aanvallen en dreigingen

- **Risicoanalyse:**

  -> op basis van risicoanalyse kunnen maatregelen genomen worden

  -> dit heeft ook een economische kant: kosten-batenanalyse

  -> cybersecurity kent een grote diversiteit aan daders en typen dreigingen dan bijvoorbeeld terrorisme

  -> de beweegredenen van daders zijn vaak verschillend, en de doelwitten lopen verder uiteen

- **Bescherming vitale Structuur:**

  -> vitale infrastructuur-bescherming is een gespecialiseerder aspect van cybersecurity

  -> onveiligheid kan grote (fysieke) schade opleveren

  -> je kan dan denken aan: energie, telecommunicatie en ICT, voedsel, gezondheid, financiële sector, openbare orde, veiligheid en transport

- **Cyberwar:**

  -> betreft het inzetten van internettoepassingen om oorlogshandelingen te verrichten?

  -> storen van de communicatie van de tegenstander om ondersteuning te bieden bij een aanval met klassieke wapens

  -> cyberwar is een bredere term, betreft niet alleen cyberaanvallen maar okk cyberverdediging

  -> bij dezelfde handeling kunnen verschillende motieven en daders een rol spelen

  -> is de dader een andere staat, of een baldadige puber? Dit levert juridische problemen op

- **Cyberspionage:**

  -> wordt zowel door bedrijven als staten gebruikt vanuit politieke en economische motieven

  -> binnen het internationale recht is spionage toegestaan, maar cyberspionnen kunnen op grond van het strafrecht beschuldigd worden

10.3 DREIGINGEN

- **Er zijn drie soorten cybersecuritydreigingen:**
    1. Informatiegerelateerde dreigingen
    2. Systeemgerelateerde dreigingen
    3. Indirecte dreigengen

-> Informatiegerelateerde dreigingen:

-> intentie van de dader is informatie verkrijgen danwel misbruiken danwel publiceren danwel veranderen

-> het CIA-principe is dat de nadruk ligt op vertrouwelijkheid en integriteit van informatie

-> voorbeeld: het inzetten van persoonsgegevens voor identificatiedoeleinden, zoals fraude met internetbankieren: de dader komt tussen de klant en de bank in te staan (man-in-the-middle-attack). Het slachtoffer kan totaal niet betrokken zijn, zoals bij een drive-by-download waarbij het bezoeken van een website al kan leiden tot een geïnfecteerde computer. Het slachtoffer kan ook meer betrokken zijn, wanneer hij een link opent in een phishing-mail

-> juridische maatregel: de meldplicht datalekken is sinds 1 januari 2016 van kracht. Indien een datalek niet tijdig wordt gemeld, kan de AP boetes opleggen tot €810.000 of 10% van de jaaromzet. **Drie voordelen:**

1. **Slachtoffers worden op de hoogte gebracht dat hun gegevens zijn gelekt**
2. **Het geeft organisaties een stimulans om hun informatie + systemen goed te beveiligen**
3. **Er kan data vergaard worden over de aard en omvang van het datalekkenprobleem**

-> Systeemgerelateerde dreigingen:

-> intentie van de dader is het verstoren van de bedrijfsorganisatie

-> het CIA-principe is dat availability hier centraal staat

-> voorbeeld: DDoS-aanvallen, vanuit welke hoek de dreiging komt, is moeilijk vast te stellen. DDoS-aanvallen kun je volgens Engelfriet nooit 100% voorkomen, je kan alleen de impact beperken

-> volgens Boele Staal is een DDoS aanval overmacht, waardoor er geen sprake kan zijn van waardecompensatie

-> banken dienen in elk geval een grotere mate van zorgvuldigheid in acht te nemen dan andere organisaties

-> Indirecte dreigingen:

-> dit zijn de neveneffecten van 1 en 2 (spill-over effect). Anderen die niet primair doelwit zijn, ervaren toch de gevolgen

-> **Dreigersgroepen:**

Vooral de diversiteit aan daders onderscheidt cybersecurity van andere veiligheidsdomeinen, zoals de bestrijding van terrorisme. 4 pure dreigersgroepen zijn:

-> hacktivisten (intentie: ideologische activistische doeleinden)

-> beroepscriminelen (intentie: financieel gewin)

-> terroristen (intentie: angst zaaien)

-> script-kiddies (is slechts een uitvoerende groep, weinig technische kennis)

-> verder zijn er nog staten en private instellingen: deze groepen kunnen zowel dreigersgroep als doelwit zijn

10.4 STRATEGIEËN EN ORGANISATIES

Steeds meer landen ontwikkelen een cybersecuritystrategie. Ook de EU. Enkele overeenkomsten:

1. Noodzaak voor de bevordering van meer coördinatie binnen de overheid op beleids- en operationeel niveau
2. Noodzaak voor het versterken van publieke-private samenwerking
3. Het bevorderen van internationale samenwerking
4. Het respect voor fundamentele rechten (privacy, vrijheid van meningsuiting en vrijhijd van informatie)

- **Nationale cybersecuritystrategie:**

  -> eerste deel legt primair de focus op de analyse van het probleem en het uiteindelijke doel van de strategie. Het tweede deel zet een aantal actielijnen uiteen en geeft aan waar de prioriteiten op het gebied van cybersecurity moeten liggen. Het uiteindelijke doel van de strategie is de versterking van de digitale veiligheid om tevens het vertrouwen in het internet te bevorderen

- **Organisaties:**

  -> de betrokkenheid van verschillende spelers heeft geleid tot de uitdaging om verantwoordelijken, bevoegdheden en verplichtingen op de juiste manier te beleggen en coördineren. Mede door het introduceren van ‘nieuwe’ organisaties ontstaat het risico van een crowded policy space

10.4.1 de situatie in België:

-> het centrum voor cybersecurity België (CCB) is het nationale centrum voor cyberveiligheid in belgië

-> doel van de CCB is het suupervisen, coördineren en het waken over de toepassing van de Belgische strategie omtrent cyberveiligheid.

- **Volgens de site is de onderverdeling als volgt:**

  -> voor de uiutvoering van zijn opdrachten doet het CCB een beroep op de administratieve en logistieke ondersteuning van de Federale Overheidsdienst Kanselarij van de Eerste Minister

  -> het centrum voor cybersecurity België zorgt als centrale autoriteit voor de cyberveiligheid in België.

    -> het zal een nationaal Cyber Security beleid opstellen en alle betrokken diensten in België aanzetten om een gepaste en geïntegreerde inspanning te leveren

  -> het CCB neemt van de FOD informatie- en communicatietechnologie het beheer over van de dienst **Computer Emergency Response Team (CERT)** voor het opsporen, het observeren en het analyseren van online veiligheidsproblemen alsook het permanent informeren daarover van de gebruikers

- **Als nationale autoriteit heeft het CCB als opdracht:**

  -> opvolgen en coördineren van en toezien op de uitvoering van het Belgisch beleid ter zake

  -> vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren

  -> de coördinatie verzekeren tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector

  -> formuleren van voorstellen tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid

  -> in samenwerking met het coördinatie- en crisiscentrum van de regering, het crisisbeheer bij cyberincidenten verzekeren

  -> opstellen, bevrijden en toezien op de uitvoering van standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen

-> coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak

-> coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen

-> informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen

- **Waarden:**

-> Het CCB hanteert volgende waarden:

-> **Integratie:** het CCB draagt bij tot een gecoördineerde en geïntegreerde aanpak van de nationale cyberveiligheid

-> **Responsabilisering:** het CCB responsabiliseert betrokken diensten en ondersteunt ze

-> **Evenwicht:** het CCB bewaart het evenwicht tussen veiligheid en de fundamentele rechten, waarden en noden van de moderne samenleving

-> **Innovatie:** het CCB stimuleert de ontwikkeling van nieuwe ideeën en mogelijkheden die de cybersecurity in België en in de wereld kunnen verbeteren

-> **Integriteit:** het CCB handelt eerlijk en eervol

-> de FOD Kanselarij van de Eerste Minister is de federale overheidsdienst die de eerste minister steunt bij de voorbereiding, de coördinatie en de iutvoering van het regeringsbeleid.

-> de kanselarij informeert over de beleidsbeslissingen van de regering en draagt België uit als kwaliteitsmerk in de wereld

10.4.2 de situatie in België en Nederland

- De minister van veiligheid en justitie is coördinerend bewindspersoon voor cybersecurity en de nationale veiligheid.
- De **Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV**, is een organisatie onder de verantwoordelijkheid van het ministerie van veiligheid en justitie) richt zich op de bescherming en de weerbaarheid van de vitale sectoren
- Binnen de NCTV fungeert het **Nationaal Cyber Security Centrum (NCSC)** als informatieknooppunt en expertisecentrum voor cybersecurity
- De cybersecurity raad geeft gevraagd en ongevraagd advies aan zowel de regering als private partijen over ontwikkelingen op het gebied van cybersecurity
- In de bancaire sector komt het ministerie van financiën in beeld, bij overheidsaangelegenheden het ministerie van binnenlandse zaken, en natuurlijk het ministerie van defensie

10.4.3 EU-initiatieven

- Al sinds 2004 is **ENISA, het Europees Agentschap voor netwerken en informatiebeveiliging,** actief op het terrein van digitale veiligheid. ENISA moet er op toezien dat binnen de EU problemen rond netwerkveiligheid worden voorkomen, beheerst en opgelost
- De richtlijn aanvallen op informatiesystemen is inmiddels geïmplementeerd
- De strafbaarstelling van computercriminaliteit is aangescherpt
- België en Nederland was in 2015 gastheer van de Global Conference on Cyberspace. Het probleem wordt steeds serieuzer aangepast

- **CONCLUSIE:**

  -> landen zijn steeds meer bezig nationale cybersecuritystrategieën te ontwikkelen

  -> cybersecurity kent haar wortels grotendeels in informatiebeveiliging

  -> cybersecurity is echter een breder en omvattender terrein dan informatiebeveiliging

  -> in het bijzonder aangezien het fenomeen zich uitstrekt over meerdere belangen en domeinen, waaronder eventuele conflicten tussen staten in de vorm van cyber war

  -> deze diversiteit wordt weergegeven in het palet aan dreigingen, waarmee verschillende partijen, van individuele gebruuikers tot aan overheidsinstanties en vitale bedrijven, worden geconfronteerd

  -> het is van ettentieel belang om na te gaan welke dreiging het meest van toepassing is op welke partij, zodat daarvoor de juiste middelen ingeschakeld kunnen worden om schade te voorkomen dan wel te beperken

  -> Incidenten, van DigiNotar tot de aanvallen op de dienstverlening van banken, hebben de dreiging concreet gemaakt en tevens de urgentie voor actie op het gebied van recht en beleid vergroot

10.6 ALGEMENE VERORDENING GEGEVENSBESCHERMING (GENERAL DATA PROTECTION REGULATION)

-> de Europese unie start een nieuw tijdperk van regels voor gegevensbeheer, deze GDPR-regels vervangen het eerdere gegevensbeschermingsmandaat van de EU, de AVG (GDPR in het engels) is aangenomen in april 2016 en was in mei 2018 volledig van kracht

-> cybersecurity en de AVG zijn dan ook uit hetzelfde hout gesneden: de gemeenschappelijke deler is data management

-> de nieuwe wet zal zowel een grotere uniformiteit bieden aan gevoelige gegevensbehandeling in de EU als betere verwerking van persoonlijke gegevens die voor niet-persoonlijke doeleinden wordt verwerkt

-> hetzelfde voorschrift: dat een levend persoon een fundamenteel recht heeft op zijn eigen datastromen, valt onder de AVG

-> net als bij de vorige regeling voor de gegevensverordening worden persoonsgegevens geacht gegevens te zijn die – direct of indirect – op iedere redelijk mogelijke wijze kunnen worden gebruikt voor het identificeren van een persoon

-> als onderdeel van haar inspanningen om uniformiteit in de EU te creëren, is de AVG automatisch van kracht in de EU-lidstaten zonder de aanneming door de eigen wetgevers van de lidstaten is vereist.

-> er zijn bepaalde uitzonderingen voor lidstaten om gegevensbehandeling in specifieke omstandigheden te bepalen, zoals rechtshandhaving en gevestigd algemeen belang

- **Wat is de bedoeling van de AVG?**

-> benadrukt het belang van een veilige bedrijfsuitvoering

-> gegevensverwerking moet de persoonlijke gegevens beter beschermen, en elke beheerder moet de juiste documentatie en beleid ter plaatse hebben om naleving vast te stellen

-> naast de benodigde beschermingsprocessen, verleent de AVG ook de betrokken grote controle over hun eigen gegevens

-> bv, elke onderneming die omgaat met persoonsgegevens moet voldoen aan de verzoeken van een betrokkene voor zijn eigen gegevens en dient de gevraagde gegevens in een verbruiksformaat te verstrekken

-> sterke invloed op de digitale privacy aan beide kanten van de oceaan. Zelfs bedrijven zonder fysieke aanwezigheid op EU-grondgebied kunnen worden getroffen.

-> stelt haar bereik vast door elke organisatie die goederen of diensten aanbiedt aan EU-onderdanen en/of gegevens voor EU-onderdanen te omvatten

-> niet naleven van het statuut kan resulteren in zware boetes en restitutie tot 4% van de wereldwijde inkomsten in sommige gevallen

-> wanneer een betrokkene schade kan bewijzen die voortvloeit uit een inbreuk op de AVG heeft hij het recht om terugbetaling van de gegevensbeheerder en/of verwerker te vragen

-> door niet-naleving bestaat er ook risico op administratieve boetes, afhankelijk van het type inbreuk kunnen boetes oplopen tot €20 miljoen of 4% van de wereldwijde omzet (welke hoger blijkt te zijn) en €10 miljoen of 2% van de wereldwijde omzet (naargelang het groter is)

-> de hogere aansprakelijkheid wordt toegepast op niet-naleving met betrekking tot de basisprincipes van de AVG, gegevensrechten van onderdanen, internationale overmaking, verplichtingen die door de wetgeving van de lidstaten zijn vastgesteld en de beslissing van een toezichthouder

- **Wat betekent de AVG voor personen en bedrijven?**

  -> verhoogt de verwachting over de privacy van gegevens en de verplichting van organisaties om de vastgestelde cybersecurity praktijken na te leven

  -> vergroot bereik: in de EU gevestigde bedrijven en bedrijven die zich richten op de EU-onderdanen en/of gegevens van EU-onderdanen verwerken zijn onderworpen aan de nieuwe verordening

  -> aansprakelijkheid: de gegevensbescherming moet standaard zijn. Processen moeten worden onderworpen privacy impactbeoordelingen en goed gedocumenteerd zijn. Processors – niet alleen controllers – hebben ook directe verplichtingen met betrekking tot de bescherming van de persoonlijke levenssfeer

  -> toestemming en gegevensrecht: toestemming moet expliciet en beperkt zijn. Personen hebben het recht op verzoek van hun gegevens, dat verzoek in te trekken en vergeten te worden

  -> melding van inbreuk op gegevens: kennisgeving aan de toezichthoudende autoriteit dient binnen de 72 uur vanaf de ontdekking te worden gedaan, behalve in gevallen waarin een schending de rechten en vrijheden van een persoon meest waarschijnlijk niet zal schaden

  -> snelle kennisgeving aan de betrokkenen is ook vereist. Uitzonderingen op de kennisgeving van de gegevens van de betrokkene zijn wanneer de persoonsgegevens onbegrijpelijk zijn (bijvoorbeeld gecodeerd) er geen groot risico van schade bestaat van de rechten en vrijheden van de betrokkene, en wanneer de kennisgeving een onevenredige inspanning inhouden

-> boetes / beoordeling: boetes voor de meest voorkomende administratieve misdrijven bedragen €20 miljoen of 4% van de wereldwijde omzet (al naargelang welke groter is) personen die zijn getroffen door onjuiste omgang met gegevens kunnen restitutie vragen bij de rechtbank

-> gegevensoverdrachten: gegevensoverdrachten buiten de EU en specifieke geautoriseerde landen en internationale organisaties zijn toegestaan zolang de data controller of processor beveiligingen heeft genomen overeenkomstig met de AVG

-> Organisaties zullen degelijke beleidskaders voor cybersecurrity moeten opstellen en implementeren om cybercriminaliteit het hoofd te kunnen bieden

10.7 FRAMEWORK VOOR DE VERBETERING VD CYBERBEVEILIGING VAN VITALE INFRASTRUCTUUR

- **Het NIST CyberSecurity Framework:**

  -> dit framework iut de verenigde staten spant zich in een beleidskader te implementeren voor computerbeveiliging. Hiermee kunnen private en publieke organisaties hun capaciteiten ter voorkoming, opsporing en bestrijding van cyberaanvallen vaststellen en verbeteren

  -> dit beleidsframework blijkt uiterst suuccesvol voor alle soorten organisaties. Het geeft bedrijven een framework met de juiste handvatten om effectief met cyberbeveiliging om te gaan

  -> niet specifiek gericht op bedrijven in de VS, het is van toepassing op alle organisaties en op alle soorten organisaties

  -> is opgesteld door het **US National Institute of Standards and Technology** in 2014 en wordt ieder jaar aangepast en verbeterd. Het helpt organisaties om pro-actief aan de slag te gaan met risicomanagement in cyberbeveiliging

  -> de vitale infrastructuur omvat publieke en particuliere eigenaars en exploitanten, en andere entiteiten die een rol spelen bij het beveiligen van de infrastructuur van de Natie

10.7.1 wat is vitale infrastructuur?

- **Vitale infrastructuur heeft betrekking op processen, systemen, faciliteiten, technologieën, netwerken, activa en diensten die essentieel zijn voor de gezondheid, veiligheid of economisch welzijn van burgers en het effectief functioneren van de overheid**

  -> bepaalde processen zijn zo vitaal voor de samenlevingdat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid

  -> deze processen vormen de vitale infrastructuur

  -> het grootste deel van de vitale infrastructuur is in handen van private partijen.

  -> De beoordeling of een proces kritisch is wordt gemaakt op basis van een aantal impactcriteria: economische schade, fysieke schade, sociaal-maatschappelijke schade en cascadegevolgen

  -> de onderdelen van elke vitale infrastructuuuursector vervullen functies die worden ondersteund door **informatietechnologie (IT)** en **industriële controlesystemen (ICS)**

  -> aangezien ICS en de gegevens die worden geproduceerd in ICS-operaties in toenemende mate gebruikt worden om kritieke diensten te leveren en bedrijfsbeslissingen te ondersteunen, dient rekening te worden gehouden met de mogelijke effecten van een cybersecurity-incident op de bedrijfsactiviteiten, de activa, de gezondheid en veiligheid van individuen en de omgeving

  -> om cyberveiligheidsrisico's te beheren, is een duidelijk begrip van de business drivers (de succesproducten) van de organisatie en veiligheidsoverwegingen die specifiek zijn voor het gebruik van IT en ICS vereist

  -> omdat het risico van elke organisatie uniek is, zal het gebruik van IT en ICS uniek zijn voor de tools en methoden om de door het framework beschreven resultaten te bereiken

  -> voor het erkennen van de rol, die de bescherming van de persoonlijke levenssfeer en burgerlijke vrijheden speelt bij het creëren van meer publiekelijk vertrouwen, is vereist dat het framework een methode bevat om individuele privacy en burgerrechten te beschermen wanneer vitale infrastructuurorganisaties cyberveiligheidsactiviteiten uitvoeren

  -> de methode is onderworpen om dergelijke processen aan te vallen en begeleiding te geven om het beheer van privacyrisico's te vergemakkelijken in overeenstemming met de aanpak van een organisatie op het gebied van cyberveiligheidsrisicobeheer

  -> integratie van privacy en cybersecurity kan organisaties ten goede komen door het vertrouwen van klanten te vergroten, waardoor meer gestandariseerde informatie kan worden gedeeld

-> om de uitbreidbaarheid te waarborgen en technische innovatie mogelijk te maken, is het framework technologisch neutraal. Dit wil zeggen dat het framework is gebasseerd op een verscheidenheid aan bestaande standaarden, richtlijnen en praktijken om het mogelijk te maken voor vitale infrastructuuurprovidors om veerkracht te krijgen

-> door te vertrouwen op die standaard normen, richtsnoeren en praktijken die door de sector zijn ontwikkeld, beheerd en geüpdatet, zullen de instrumenten en methoden beschikbaar zijn om de framework-uitkomsten te bereiken, over de grenzen heen te reiken, de wereldwijde aard van cyberveiligheidsrisico's zullen worden erkend en ontwikkeld met de technologische vooruitgang en de bedrijfsvereisten

-> Marktconcurrentie bevordert ook snellere verspreiding van deze technologieën en praktijken en het realiseren van veel voordelen door de belanghebbenden in deze sectoren

-> Op basis van richtlijnen en praktijken, biedt het framework in een gemeenschappelijke classificatie en mechanisme om:

-> de huidige houding tegenover cybersecurity te omschrijven

-> hun doelstaat (land) voor cybersecurity te omschrijven

-> kansen voor verbetering te identificeren en prioriteren in het framework van een continu en herhaalbaar proces

-> de vooruitgang in de richting van de doelstaat beoordelen

-> te communiceren tussen interne en externe stakeholders over cyberveiligheidsrisico's

-> Het framework is een aanvulling, geen vervanging van het risicobeheerproces en het cyberveilighheidsprogramma van een organisatie

-> de organisatie kan zijn huidige processen en het framework gebruiken om kansen te identificeren om het beheer van het cyberveiligheidsrisico te versterken en re communiceren, terwijl het afstemt op de industriepraktijken

-> als alternatief kan een organisatie zonder een bestaand cybersecurityprogramma het framework gebruiken als referentie om er één te vestigen

-> als straks om jouw advies wordt gevraagd door het bedrijfsleven en/of de overheid, kun je onderstaande framework inzetten voor de implementatie van een cybersecurityprogramma

-> de implementatie van het framework is geen simpele opgave en je kunt het niet alleen doen. Je hebt de volledige medewerking van de organisatie nodig en medewerkers binnen de organisatie die dit samen met jouw op touw gaan zetten

-> aangezien het framework niet bedrijfstakspecifiek is, is de gemeenschappelijke classificatie van normen, richtlijnen en praktijken die het biedt ook niet landspecifiek

-> het framework kan bijdragen tot het ontwikkelen van een gemeenschappelijke taal voor internationale samenwerking op het gebied van kritieke infrastructuuur cyberveiligheid

10.9 DE EFFECTEN VAN AFWEERSYSTEMEN OP HET INTERNET

- Een systeem binnendringen wordt gedinieerdals'illegally gaining acces to one or more computer systems after exploiting security vulnerabilities or defeating a security barrier'. Oftewel: illegaal toegang verkrijgen tot één of meer computers nadat misbruik is gemaakt van de kwetsbaarheden van beveiliging of nadat een beveiligingsobstakel uit de weg is geruimd.
- Onlangs zijn bij 580 IT-medewerkers enquêtes afgenomen, daaruit volgt dat ongeveer 90% van de Amerikaanse bedrijven meerdere malen gehackt worden.
- Resulteert in mijarden van verlies
- Zware inbreuk op de privacy
- Dit onderdeel gaat over pop-up meldingen waarin gedreigd wordt met een sanctie. Hierbij wordt gekeken naar de progressie, fresuuentie en duur van een hack (sytstem trespassing)

- Vier hoofdvragen;
    1. Kan een warning banner (melding) ervoor zorgen dat een eerste hack beïndigd wordt?
    2. Kan een melding de frequentie van het aantal hacks verminderen?
    3. Heeft een melding effect op de duur van een eerste en herhaalde hack?
    4. Tasten verschillende computerconfiguraties het effect van een melding aan tijdens een hack?

- **System Trespassing:**

-> Hacken betreft het overtreden van eigendomsregels, het 'gaining acces to property' dat niet van jou is. Hacken kan door je fysiek toegang te verlenen tot een computer, maar kan ook van op afstand met het internet. Men hackt vanwege wraak, geldelijk gewin, thrill, status, verslaving

-> hackers scannen random het internet op zoek naar open computerpoorten en gebruiken hierbij hackingsoftware die vrij te kopen is op internet.

-> de software produceert oneindig veel wachtwoorden en kijkt vervolgens met welk wachtwoord de toegang verleend kan worden.

-> nadat de toegang is verschaft kunnen hackers doen wat ze willen

-> het amerikaanse congres heeft regels hieromtrent neergelegd in de Computer Frauud and Abuse Act (1986)

- **Deterrence theory (afschriktheorie):**

  -> in utilitaristische stromingen (d.w.z. gericht op onmiddelijk nut) binnen de filosofie heeft de afschriktheorie een prominente plaats. De theorie van Beccaria en later verfijnd door Bentham (2 oprichters van de klassieke criminologie) stelt dat dreiging met straf het criminele gedrag beïnvloedt op een positieve manier. Dit omdat straf de kosten-baten vergelijking beïnvloedt (straf verhoogt de kosten)

  -> **straf moet voldoen aan 3 aspecten:**

  -> omvang: straf moet passend zijn

  -> zekerheid: straf moet zeker zijn

  -> nabijheid: straf moet direct volgen op de misdaad

  -> **afschrikking kan onderverdeeld worden in:**

  -> algemene afschrikking: afschrikking gericht op het publiek

  -> specifieke afschrikking: afschrikking gericht op de dader

  -> **kan tevens onderverdeeld worden in:**

  -> objectieve afschrikking: daadwerkelijke risico, straf, etc.)

  -> subjectieve afschrikking: perceptie van omvang, zekerheid en nabijheid)

  -> **tenslotte kan afschrikking onderverdeeld worden in:**

  -> absolute afschrikking: er volgt geen misdaad

  -> restrictieve afschrikking: de misdaad die volgt is minder ernstig of de frequentie is veel lager

  -> first-time players kunnen net als ex-plegers vanwege afschrikking een ernstige misdaad plegen

  -> er is geen statistisch onderzoek geweest waarin een direct verband blootgesteld wordt tussen afschrikking met straf en vermindering van de ernst, frequentie of duur van de criminele daad

- **Afschrikmiddelen en waarschuwingen:**

  -> meldingen kunnen een positief effect hebben (bv in het verkeer), maar ook een negatief effect (zoals bij zakkenrollen)

  -> ook zijn er criminaliteitsvormen waarop een melding totaal geen effect heeft (prostitutie)

  -> al deze studies kijken naar het effect op een melding in voorkomen van criminaliteit (occurrence), maar weinig studies kijken naar het effect van een melding op de voortgang en duur van criminaliteit (progression & duration)

  -> **een melding moet bevatten:**

    -> Welke regels worden overtreden

    -> wat de sanctie is wanneer deze regels worden overtreden

  -> **Hypotheses in dit onderzoek:**

    -> een waarschuwingsbanner kan ontmoedigen, stimuleren, of het heeft geen effect

    -> aanwezigheid van een sanctiedreiging inbreuken op een doelcomputer vermindert

    -> aanwezigheid van een waarschuuwingsbanner de duur van zowel de eerste en vervolg inbreuken op het systeem verkort

    -> grote hoeveelheid RAM en hoge bandbreedte van het computerdoelsysteem het effect van een waarschuuwingsbanner verkort op de duur van een inbreuk

    RAM: random acces memory (de mogelijkheid computerdata snel te verwerken)

    Bandbreedtecapaciteit: de hoeveelheid data die per seconde door een verbinding verstuurd kan worden

  CONCLUSIE VAN ONDERZOEKEN/EXPERIMENTEN:

    -> een melding heeft geen invloed op het wel of niet doorgaan van een hack

    -> een melding verkleint de frequentie van hacks niet

    -> verkort wel de tijd van de eerste en herhaalde hacks

    -> effect is het grootst bij computers met een lage bandwith capaciteit omdat de hack moeilijk wordt en het risico gepakt te worden groter is

    -> RAM grootte heeft geen effect op de duur van de hacks

10.10 EU-CYBERSECURITYSTRATEGIE

10.10.1 naar een open, veilig en betrouwbaar internet

- in dit onderdeel wordt het Voorstel van de commisie van 7 februari 2013 behandeld om een richtlijn in te voeren ter verhoging van het algehele niveau van beveiliging van netwerk en informatiesystemen in Europese unie
- De auteurs plaatsen kanttekeningen bij de gekozen maatregelen en de implementatie daarvan. Zij onderschrijven de noodzaak tot het treffen van maatregelen op Europees niveau
- Sluiten af met hun aanbevelingen:

  -> **7 februari 2013:** Europese Commisie publiceerde haar visie op de aanpak van informatiebeveiligingsproblemen: in de vorm van een integrale cybersecuritystrategie.

  -> **prioriteiten:** 'verhogen van digitale weerbaarheid', 'reduceren van cybercrime'

  -> ontwikkelen: europees cyberdefentiebeleid 'ontwikkelen van een internationaal beveiligingsbeleid voor cyberspace'

  -> doel: 'veilig en betrouwbare digitale omgeving', 'waarborgen van Europese rechten en kernwaarden' een belangrijk onderdeel van de strategie van de commisie wordt gevormd door een richtlijn die een hoger gemeenschappelijk niveau van beveiliging van netwerken informatiesystemen beoogt te realiseren **("NIB-Richtlijn")**

- **Informatiebeveiliging en het correct functioneren van ICT wordt nagestreefd op basis van het CIA-Model:**

  -> Confidentialiteit (confidentiality)

  -> Integriteit (integrity)

  -> Beschikbaarheid (availability)

- Kwetsbaarheden die kunnen leiden tot tekortkomingen van informatiebeveiliging kunnen verschillende oorzaken hebben:

  -> gebrekkige hardware / software

  -> onjuist gebruik van technologie (bv in de implementatie)

  -> onjuist gebruik van technologie kan ook gelegen zijn in het eindgebruik, zoals wanneer wachtwoorden uitgeleend worden

- Gevolg van het gebruik van kwetsbare producten en onjuist gebruik: informatie en de ICT zelf is kwetsbaar voor verstoring, uitval en misbruuik (vb spionage)

  -> Cybercrime hacktivisme en spionage nemen in complexiteit en aantallen toe

  -> uitval kan ook een gevolg zijn van overmacht (bv brand)

- **BELANGRIJK:** bestrijden van kwaadwillend handelen vereist andere ingrijpen dan het voorkomen van fouten bij het ontwikkelen en gebruik van ICT producten. De oorzaak van beveiligingsproblemen is noodzakelijk om de aanpak te bepalen.

10.10.2 cyberbeveiligingsinitiatieven door de EU

- De Europese commissie heeft zijn inspanningen vergroot om online Europeanen nog beter te beschermen. Het heeft een reeks wetgevingsvoorstellen aangenomen, met name op het gebied van netwerk- en informatiebeveiliging
- In periode meer dan €600 miljoen toebedeeld aan partners en het wereldwijde podium vergroot en versterkt door de politieke cyberbeveiliging in haar politieke prioriteiten te betrekken
- In juli 2016 presenteerde de commissie aanvullende maatregelen ter bevordering van de cybersecurity insustrie en de aanpak van cyberdreigingen
- De goedkeuring van de richtlijn inzake beveiliging van netwerk- en informatiesystemen **(NIS-richtlijn)** door het europes parlement in juli 2016 is een belangrijke mijlpaal naar een veilige online omgeving

- **Waarom is cybersecurity zo belangrijk?**

  -> digitale technologieën zijn de ruggengraat van onze economie geworden

  -> kritische bron van alle economische sectoren

  -> ondersteunen complexe systemen zoals financiën, gezondheid, energie en vervoer

  -> het functioneren van informatiesystemen dat vereist is

  -> door cyberincidenten kunnen de levering van electriciteit, water verstoren

  -> dreigingen kunnen uit verschillende hoeken komen: waaronder criminele, terroristische of staatsgebonden aanvallen alsmede natuurrampen en onbedoelde fouten

  -> door de digitale interne markt te voltooien, zou de economie kunnen versterken met bijna 415 miljard euro per jaar en honderd duizend nieuwe banen kunnen creëren

  -> digitale wereld moet beschermd worden tegen incidenten, kwaadaardige activiteiten en misbruik

  -> prioriteit van de commissie om deze incidenten te voorkomen en indien deze zich voordoen, deze de meest efficiënte response te bieden

- **Wat zijn de belangrijkste doelstellingen van de Commissie op het gebied van cybersecurity?**

1. **Toenemende mogelijkheden voor cyberveiligheid en samenwerking**

   -> doel is de mogelijkheden van cyberbeveiliging op hetzelfde niveau van ontwikkeling in alle EU-staten te brengen

   -> Ervoor zorgen dat de uitwisseling van informatie en samenwerking efficiënt is, ook op grensoverschrijdend niveau

2. **Van de EU een sterke speler in cybersecurity maken:**

   -> Europa moet ambitieuzer zijn om het concurrentievoordeel op het gebied van cybersecurity te bevorderen

   -> Ervoor zorgen dat Europese burgers, bedrijven, overheidsdiensten toegang hebben tot de nieuwste digitale beveiligingstechnologie die interoperabel, concurrerend, betrouwbaar zijn en de grondrechten, inclusief het recht op privacy respecteert

   -> Europese cyberbeveiligingsindustrie een stimulans geven

3. **Integratie van cybersecurity in EU-beleid:**

   -> doel is vanaf de start cyberbeveiliging in de beleidsinitiatieven van de EU te integreren, met name betrekking tot nieuwe technologieën en opkomende sectoren, zoals connected cars, slimme netwerken, the intenet of things

4. **Wat doet de commissie om cybersecurity te vergroten?**

   -> de commissie heeft verschillende initiatieven voorgelegd en draagt bij tot een aantal belangrijke maatregelen

10.10.3 strategieën vanuit de EU

- De commissie en European External Action Service hebben in 2013 de EU-cyberbeveiligingsstrategie gelanceerd.
- de strategie schetst de principes die de EU-actie op dit gebied zullen begeleiden, bv over het belang van toegang op het internet en bescherming van de grondrechten online. -> **Vijf prioriteiten:**
  a. Toenemende cyberbestendigheid
  b. Het ontwikkelinsbeleid van de EU inzake cyberverdediging en capaciteiten in verband met het gemeenschappelijk veiligheids- en defensiebeleid **(GVDB)**
  c. Drastisch verminderen van cybercriminaliteit
  d. Ontwikkeling van industriële en technologische middelen voor cybersecurity
  e. Opzetten van samenhangend internationaal cyberspacebeleid voor de EU en de bevordering van kernwaarden van de EU

- **Europese agenda voor cyberveiligheid (2015):**

  Cybercrime vereist een gecoördineerd antwoord op Europees niveau, daarom stelt de Europese agenda voor veiligheid de volgende acties vast:

  -> hernieuwde nadruk leggen op implementatie van bestaand beleid op het gebied van cybersecurity, aanvallen op informatiesystemen, en bestrijding van seksuele uitbuiting van kinderen

  -> herziening en mogelijk uitbreiding van de wetgeving ter bestrijding van fraude en vervalsing van niet-contante middelen van betalingen teneinde rekening te houden met nieuwere vormen van misdaad en namaak van financiële instrumenten

  -> herziening van belemmeringen in criminele onderzoeken over cybercriminaliteit, met name over kwesties van bevoegde jurisdictie en regels over toegang tot bewijs en informatie

  -> het vergroten van acties voor capaciteitsopbouuw krachtens instrumenten van buitenlandse hulp

- **Strategie voor digitale interne market:**

  -> vertrouwen en veiligheid zijn ettentieel om de voordelen uit de digitale economie te kunnen behalen

  -> daarom is de strategie voor digitale interne markt gepresenteerd en omvat een publiek-private samenwerking **(PPP)** over cybersecurity

  -> **partnerschap is ondertekend door de Commissie en de Europese Cyber Security Organisation (ESCO):**

    -> een op de bedrijfstakgerichte vereniging, die een grote verscheidenheid aan belanghebbenden omvat zoals grote bedrijven, kleine en middelgrote ondernemingen, startende ondernemingen, onderzoekscentra, universiteiten, eindgebruikers, exploitanten, clusters en verenigingen, alsmede overheden

    -> doel van dit partnerschap is het concurrentievermogen van Europa te stimuleren en de marktfragmentatie van de cyberveiligheid te verkleinen door innovatie

    -> het vertrouwen tussen de lidstaten en industriële actoren te versterken, en de vraag- en aanbodsectoren voor producten en oplossingen voor cybersecurity te ondersteunen

    -> dit partnerschap zal ettentieel zijn voor het structureren en coördineren van de digitale beveiligingsindustrie in Europa.

    -> het omvat een breed scala aan actoren, van innovatieve MKB tot producenten van componenten en apparatuur, vitale infrastructuurexploitanten en onderzoeksinstituten

-> het initiatief zal de middelen van de EU, nationale, regionale en particukiere sectoren, met inbegrip van onderzoeks- en innovatiefondsen, inzetten om investeringen te verhogen

-> Uiteindelijk helpt het partnerschap met de volgende zaken:

a. Induustriële en publieke middelen verzamelen om innovatie te leveren tegen een gezamenlijk overeengekomen strategisch onderzoeks- en innovatieplan
b. Gericht zijn op gerichte technische prioriteiten die gezamenlijk met de industrie zijn vastgesteld
c. De impact van de beschikbare middelen maximaliseren
d. Zichtbaarheid geven op de Europes onderzoeks- en innovatie-exxcellence op het gebied van cybersecurity

-> het partnerschap wordt ondersteund door EU-fondsen die afkomstig zijn uit het **Horizon 2020 Research and Innovation Framework Programme (H2020)** met een totale investering van maximaal €450 miljoen tot 2020

-> het partnerschap bevat een aantal maatregelen gericht op:

a. Samenwerking in Europa versterken: de Commissie moedigt aan om de samenwerkingsmechanismen van de **NIS-richtlijn (Network and Information Security – Europese richtlijn voor cybersecurity)** optimaal te benutten en de manier waarop zij samenwerken om zich voor te bereiden op een grootschalig cyberincident, te verbeteren
b. Ondersteuning van de opkomende interne markt voor cybersecuritydiensten en –producten in de EU
c. Het opzetten van een contractueel publiek-particulier partnerschap (PPP) met de industrie om de cybersecuritycapaciteiten in bedrijven te vergroten en innovatie in de EU.

10.10.4 EU-wetgeving

- **Richtlijn inzake netwerk- en informatiebeveiliging:**

-> in 2013 heeft de commissie de richtlijn voor de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn) voorgesteld om een hoog gemeenschappelijk niveau van cybersecurity in de EU te waarborgen

-> onderhandelaars van det Europees Parlement, de Raad en de Commisie hebben overeenstemming bereikt over de tekst

-> de lidstaten hadden vervolgens 21 maanden om de richtlijn in hun nationale wetgeving op te nemen en 6 maanden om exploitanten van essentiële diensten vast te stellen

-> De richtlijn is gebaseerd op drie hoofdpeilers:

-> Ervoor zorgen dat de lidstaten bereid zijn om hen op passende wijze te voorzien, bv via een **computerbeveiliging Incident Response Team (CSIRT)** en een bevoegde nationale NIS autoriteit

-> Het waarborgen van samenwerking tussen alle lidstaten door een samenwerkingsgroep op te zetten om strategische samenwerking en uitwisseling van informatie tussen de lidstaten en een "CSIRT-netwerk", te ondersteunen en te vergemakkelijken teneinde snelle en effectieve operationele activiteiten te bevorderen, samenwerking op speciefieke cybersecurity incidenten en informatie over risico's delen

-> De waarborgen van een veiligheidscultuur over sectoren die van vitaal belang zijn voor economie en samenleving. Bedrijven met een belangrijke rol voor de samenleving en de economie die door de lidstaten geïdentificeerd zijn als exploitanten van essentiële diensten in het kader van de NIS-richtlijn, moeten passende veiligheidsmaatregelen nemen en ernstige incidenten aan de bevoegde nationale autoriteit meededelen.

-> deze sectoren omvatten energie, vervoer, water, bankwezen, financiële marktinfrastructuur, gezondheidszorg en digitale infrastructuur

- Ook belangrijke dienstverleners (zoekmachines, cloud computing services en online marktplaatsen) moeten voldoen aan de beveiligings- en kennisgevingsvereisten. Soortgelijke eisen gelden reeds voor telecomoperators en internetdienstverleners via het EU-regelgevingskader voor telecommunicatie

- **Wetgevende acties om cybercriminaliteit te bestrijden:**

-> een richtlijn betreffende aanvallen op informatiesystemen, die gericht zijn op het aanpakken van grootschalige cyberaanvallen door de lidstaten te verplichten de nationale wetgeving inzake cybercriminaliteit te versterken en strengere strafrechtelijke sancties in te voeren

-> de commissie controleert momenteel de uitvoering ervan

- **heeft betrekking tot:**

-> een richtlijn ter bestrijding van de seksuele uitbuiting van kinderen online en kinderpornografie

-> kaderbesluit ter bestrijding van fraude en namaak van niet contante betalingsmiddelen

10.11 NETWERKEN / ORGANISATIES

- **Het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA):**

  -> opgericht in 2004 om bij te dragen tot het algemene doel om een hoog nieveau van netwerk- en informatiebeveiliging binnen de EU te waarborgen

  -> ENISA helpt de Commissie, de lidstaten en het bedrijfsleven zich te adresseren, te reageren en vooral om NIS-problemen te voorkomen

  -> De belangrijkste activiteiten van ENISA zijn:

    -> verzamelen en analyseren van gegevens over beveiligingsincidenten in Europa en opkomende risico's

    -> het bevorderen van risicobeoordelingsmethodes en risicobeheersingsmethoden om het vermogen om informatiebeveiligingsgevaar te behandelen en te verbeteren

    -> het runnen van pan-Europese cyberoefeningen

    -> ondersteuning van samenwerking op het gebied van **computer-noodrespons teams (CERT's)** in de lidstaten

    -> bewustwording en samenwerking tussen verschillende actoren op het gebied van informatiebeveiliging

- **Het EU Computer Emergency Response Team (CERT-EU):**

  -> opgericht in 2012 met het doel effectief en efficiënt antwoord te geven op informatiebeveiligingsincidenten en cyberdreigingen voor de EU-instellingen, agentschappen en instanties

  -> CERT-Eu werkt ook samen met andere CERT's in de lidstaten en daarbuiten

- **Het Europolcentrum voor cybercriminaliteit (EC3):**

  -> in 2013 opgericht als integraal onderdeel van Europol en is een brandpunt geworden bij het bestrijden en voorkomen van **grensoverschrijdende cybercriminaliteit door:**

  -> te dienen als centrale hub voor criminele informatie en intelligentie

  -> operaties en onderzoeken van de lidstaten te ondersteunen door middel van operationele analyse, coördinatie en expertise

  -> het bieden van strategische analyseproducten

  -> samen te werken met cybercriminele wetstoepassingsdiensten, de paticuliere sector, universitaire en andere non-law enforcement partners (internetbedrijven, financiële sector, computer emergency response teams) om de samenwerking tussen hen te verbeteren

  -> ondersteuning van opleiding en capaciteitsopbouw in de lidstaten

  -> het verstrekken van hoog gespecialiseerde technische en digitale forensische ondersteuningscapaciteiten aan onderzoeken en operaties

  -> vertegenwoordiging van de EU-rechtshandhavingsgemeenschap op het gebied van gemeenschappelijk belangen (vereisten van research & development, internetbeheer, beleidsontwikkeling)

10.12 EU-FINANCIERING

- **Onderzoek en innovatie:**

  -> onderwerpen zoals betrouwbare netwerk- en dienstinfrastructuur, cryptologie en geavanceerde biometrie werden behandeld in het **7Th Framework Programme (FP7) and the Competiveness and Innovation Programme (CIP)**

  -> KP7 heeft €50 miljoen geïnvesteerd in cybercriminaliteitsprojecten die onderwerpen zoals de cybercrime-economie, risicoanalyse voor infrastructuurbeveiliging, witwassen van geld en speciefieke road-mapping acties(stappenplan) behandelen

  -> van 2014-2016 heeft de EU €160 miljoen geïnvesteerd in het kaderprogramma **Horizon 2020 Research and Innovation Framework Programme (H2020)** in onderzoeks- en innovatieprojecten voor cyberveiligheid

-> EU zal ook tot €450 miljoen van de financiering van H2020 investeren om cyberveiligheidsonderzoek en –initiatieven uit te voeren in het kader van het contractuele publiek-private partnerschap inzake cybersecurity

- **Digital Security Strand:**

  -> richt zich op het vergroten van de beveiliging van actuele applicaties, diensten en infrastructuur door de modernste beveiligingsoplossingen of processen te integreren

  -> waarbij de opbouw van leidende markten en marktincentives in Europa wordt ondersteund

  -> het doel is om digitale beveiligingsintegratie in de applicatie domeinen te waarborgen

- **Fighting Crime and Terrorism Strand:**

  -> concentreert zich op het vergroten van de kennis van het fenomeen cybercrime

  -> speciefieke elementen daarvan, de economie en de middelen voor de rechtshandhavingsautoriteiten om het efficiënter te bestrijden en daders te vervolgen met meer solide bewijzen uit gespecialiseerde forensische activiteiten

- **Infrastructuren:**

  -> Europese Structuur- en Investeringsfonds (ESI):

  -> ESI-fondsen kunnen investeringen in beveiliging en gegevensbescherming financieren om de interoperabiliteit en interconnectie van digitale infrastructuren, elektronische identificatie, privacy en vertrouuwensdiensten te verbeteren

  -> cybersecurity is een van de gebieden die worden ondersteund krachtens de **Digital Service Infrastructures (DSI's)** stroom binnen de **Connecting Europe Facility (CEF)**

  -> de gefinancieerde projecten implementeren trans-Europese digitale diensten op basis van oplossingen zoals e-identificatie en interoperabele gezondheidsdiensten

  -> een van de doelstellingen is het bereiken van grensoverschrijdende samenwerking op het gebied van cybersecurity, het vergroten van de veiligheid en daarmee het vertrouwen in grensoverschrijdende elektronische communicatie

- **Projecten tegen cybercriminaliteit:**

  ->De Commisie steunt de strijd tegen cybercriminaliteit door het Cybercrime Center (EC3) van Europol (personeel en operationele kosten) te financieren en door middel van cybercriminaliteitsprojecten te financieren zoals:

  -> het programma voor preventie en bestrijding van criminaliteit

  -> het intern beveiligingsfonds (ISF) als opvolger van ISEC

  -> concrete acties die via dit instrument worden gefinancierd kunnen een breed scala aan initiatieven omvatten, zoals het opzetten van IT-systemen, het verwerven van operationele apparatuur, het bevorderen en ontwikkelen van opleidingsprogramma's en het verzekeren van administratieve en operationele coördinatie en samenwerking

- **Capaciteitsopbouw in derde landen:**

  -> doel is met de derde landen een verbintenis voor capaciteitsopbouw aan te gaan, de doelstellingen zijn de technische vaardigheden van derde landen te verhogen en doeltreffende juridische kaders op te zetten om cybercriminaliteit tegen te gaan

  -> tegelijk verbeteren van hun capaciteit voor effectieve internationale samenwerking op deze gebieden

  -> gefinancierd door **Instrument contributing to Stability and Peace (IcSP),** waarbij cyberveiligheid en de bestrijding van criminaliteit sinds 2013 met prioriteit zijn gefinancierd

  -> in speciefieke regio's ook andere instrumenten, waaronder **Europees nabuurschapsinstrument (ENI),** dat wordt ingezet om landen van het Oost-partnerschap (Armenië, Azerbeidzjan, Wit-Rusland, Georgië, Moldavië, Oekraïne) te helpen bij het vaststellen van strategische prioriteiten in verband met de strijd tegen cybercrime

  -> **het Instrument van Pretoetreding (IPA)** financieerd een nieuwe actie van €5 miljoen om de landen in Zuid-oost Europa en Turkije te helpen samen te werken aan cybercriminaliteit

- **Internationale activiteiten:**

  -> The European External Action Service (EEAS):

  -> zorgen met de commissie ervoor dat, samen met de lidstaten, internationale acties op het gebied van cybersecurity worden gecoördineerd.

  -> Daarmee tracht de EDEO de kernwaarden van de EU te handhaven en een vreedzaam, open en transparant gebruik van cybertechnologieën te bevorderen

  -> de EDEO, de Commissie en de lidstaten voeren een politieke dialoog met internationale partners en organisaties zoals de Raad van Europa, de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE), de Noord-Atlantische Verdragsorganisatie (NAVO) en de Verenigde Naties

  -> de EDEO en de Commissie vestigen in nauwe samenwerking met de lidstaten verbanden en dialogen over internationaal cyberbeleid en beveiliging van informatie- en communicatietechnologieën met belangrijke strategische partners zoals Brazilië, Chiona, India, Japan, De Republiek van Korea en de Verenigde Staten

  -> de commissie steuunt ook de capaciteitsopbouw in derde landen