6 CRIMINALITEIT EN HET INTERNET

6.1 CRIMINELE ZAKEN OP HET INTERNET

6.1.1 dark web

-> Niet te bereiken met normale internetbrowsers als IE en chrome

-> enkel met een speciaal geconfigureerde browser als the onion router -> TOR-browser

-> dmv Tor kun je anoniem surfen op het internet en blijf je onopgemerkt

-> de data die je verstuurt wordt geanonimiseerd en in verschillende lagen van versleuteling omhuld

- **Tor hidden systems:**

  -> maakt het mogelijk om anoniem websites te hosten zonder dat de locatie wordt onthuld

  -> Tor biedt dus ononimiteit voor zowel gebruikers als de mensen die de verborgen websites hosten.

- **Illegale online markten:**

  -> de meest beruchte was Silk Road, ontstaan in 2011, gehost via Tor.

  -> in 2013 ontmanteld door operatie 'Marco Polo' door homeland security

  -> tweede versie werd online gezet maar snel onderuit gehaald

  -> verweven in applicaties/forums aan de top van de infrastructuur van het internet

  -> koop- en verkoopplaatsen voor illegale goederen als wapens en drugs

  -> locatie van deze illegale markten werd verplaatst van de fysieke naar de online wereld

- **Beeldmateriaal van kindermisbruik:**

  -> Voor het internet waren dit fysieke foto's en dergelijke die pedofielen onderling met elkaar deelden

  -> het internet veranderde de wijze waarop beeldmateriaal gedeeld wordt

  -> pedofielen komen nu samen in Dark webchat platforms waar zij anoniem foto's en videos delen

  -> net zoals met illegale markten is met de komst van het dark web voor kindermisbruik niet een nieuwe vorm van criminaliteit ontstaan.

  -> maakt het voor criminelen gemakkelijker om hun praktijken uit te voeren

  -> de kosten van de criminaliteit zijn gedaald

- **Datalekken en identiteitsfraude:**

  -> in het midden van het continuuüm van cybercrime zijn vormen die een combinatie zijn van het gebruik van applicaties/platforms 'on top of the network' en het gebruik van het netwerk als een middel om criminaliteit te plegen.

  -> voorbeelden hiervan zijn datalekken en identiteitsfraude

  -> deze vormen maken gebruik van de infrastructuur van het netwerk

  -> doen daarbij ook een beroep op Dark Webapplicaties

  -> voor de komst van het internet was identiteitsfraude vooral de naam aannemen van iemand anders / stelen van paspoort/rijbewijs en id

  -> sinds de komst van het internet gaat het vooral om het stelen van de digitale identiteit

    - **Digitale identiteitsdiefstal kent 2 processen:**

    -> Cybercriminelen maken gebruik van de 'infrastructuur van het internet' door netwerk/databases te hacken om zo creditcardgegevens/inloggegevens/emailadressen etc. Te ontfutselen

    -> Het verkopen van de gestolen informatie. Dit is vaak duur en riskant, dus gebeurt dit vaak op illegale markten op het dark web

  -> persoonlijke gegevens worden steeds meer opgeslagen in databases

      Dit maakt dienstverlening/het zoeken van persoonsgegevens/winst maken gemakkelijker

  -> wanneer cybercriminelen zichzelf toegang verlenen tot een database kuunnen zij van de gehele bevolking persoonsgegevens stelen

  -> datalekken en identiteitsdiefstal is een proces dat bestaat uit twee stappen

    a. Identiteitsdiefstal wordt begaan via de infrastruuctuur van het netwerk (inbreken in een database met vertrouwelijke informatie)
    b. Zodra de aanvallers in het bezit zijn van deze info proberen ze deze kwijt te geraken op het dark web 'on top of the network'

6.1.2 ransomware

-> **combinatie van beide uiteinden van het continuüm**

a. het netwerk 'the infrastructure of the network' wordt gebruikt om malware te verzenden van apparaat A naar apparaat B
b. Om vervolgens de misdaad af te ronden en deze te verkopen via het dark web 'on top of the network'

- **Bijvoorbeeld:**

  ->een hacker hackt iemand zijn desktop/laptop en installeert geavanceerde encryptie-technologieën. Een onschuldige muisklik in een link van een email is vaak voldoende om de computer te infecteren met trojaanse paarden.

  -> criminelen krijgen hierdoor toegang tot bestanden op je PC en de oorspronkelijke gebruiker niet meer.

  -> hackers maken contact met de gebruiker door middel van een pop-up schermpje waar ze losgeld in eisen om hun bestanden terug te krijgen.

  -> betalingen dienen te worden gedaan vua anonieme valuta zoals bitcoin via een online betaling website die dan weer gehost wordt via het dark web

  -> daardoor is het zeer moeilijk om te zeggen niet te traceren door opsporingsoperaties

6.1.3 distributed denial of service attacks (DDos)

-> is een voorbeeld van een cybercrime aan het andere uiterste van het continuüm (via netwerkinfrastructuur)

-> klassieke manier om een DDoS aanval uit te voeren was een enorme lading e-mails te versturen waardoor de server van een bedrijf of overheid komt plat te liggen

-> doel van een DDoS aanval is om een bedrijf zoals een bank, instelling te verstoren

6.1.4 internet gerelateerde criminaliteit

-> **cybercrime bestaat grofweg uit twee toepassingen:**

a. Criminele activiteiten in applicaties/forums/platforms
b. Misdaad gepleegd via de infrastructuur van het netwerk

-> naast de overheid zijn er private actoren bevoegd om cybercrime te bestrijden

-> bijvoorbeeld Microsoft en IT-beveiligingsbedrijven zoals norton

-> hierbij is nog weinig samenwerking tussen de verschillende instanties

6.2 STRATEGIEËN OM CYBERCRIME TEGEN TE GAAN

6.2.1 dark web indexing

-> opsporingsinstanties hebben een poging gedaan alle websites die bestaan op het dark web te identificeren en te indexeren

-> Interpol heeft in samenwerking met IT-beveiligingsbedrijf Kaspersky onderzoeksmethoden om de contouren van het dark web te bepalen

-> naar schatting zijn er 60.000 tot 80.000 sites die door Tor verborgen worden

-> wanneer opsporingsinstanties de locaties weet van sites van illegale markten etc. Kunnen van daariut effectieve maatregelen worden genomen en de cybercriminelen opsporen

-> dark web indexing is effectief voor opsporing van cybercriminelen op illegale markten en kindermisbruik sites omdat deze sites een relatief lage 'churn rate' (bezoekers blijven langer op de site) hebben in vergelijking met andere dark websites

-> ransomware aanvallen worden waarschijnlijk niet beïnvloed door dark webindexingering

-> ransomware criminelen kunnen na een transactie weer uitwijken naar een nieuwe website

-> zij kunnen zich sneller verplaatsen en zijn hierdoor lastiger te lokaliseren

-> voor illegale markten en kindermisbruik sites is dark web indexing zeer effectief gezien het stabiele gebruik van deze websites.

-> minder grote impact het op de beperking van identiteits diefstal en DDoS aanvallen omdat deze vormen niet enkel gebruik maken van het dark web, deze zijn ook in staat om snel nieuwe sites te lanceren waardoor ze moeilijker te lokaliseren zijn.

6.2.2 ISP botnet mitigation

-> ISP's zijn Internet Service Providers, netwerkproviders die internet mogelijk maken

-> veel zijn eigendom van particulier, sommige worden beheerd door bedrijven

-> ISP's zijn knelpunten voor het internetverkeer en kan nuttig zijn voor in strijd tegen cybercrime

-> ISP's nemen contact op met gebruikers wanneer huin desktop/laptop etc. Geïnfecteerd zijn met malware dmv het internet

-> net zoals mensen heb je goede ISP's en slechte ISP's

-> Sommigen hebben hun netwerk goed beveiligd terwijl anderen hun infrastructuur laten gebruiken voor criminele activiteiten

-> ISP's kunnen botnetverkeer van dubieuze afkomst blokkeren en daarmee de ernst van SPAM en DDoS verminderen

-> bijvoorbeeld door te kijken naar onregelmatige verkeerspatronen en geïnfecteerde PC's lokaliseren

-> ze kunnen contact opnemen met geïnfecteerde gebruikers en meedenken aan een oplossing

-> ze hebben verschillende mate van effectiviteit

a. Zeer effectief: verminderen van DDoS aanvallen, SPAM mails
b. Effectief: ter voorkoming van ransomware
c. Weinig effectief: applicaties/fora op het dark web en illegale markten omdat deze cybercrime vormen niet afhankelijk zijn van botnets

Er zijn verschillende soorten cybercrime die te plaatsen zijn langs een vacuüm. Sommige criminele activiteiten vinden bovenop het netwerk plaats (applicaties/fora/websites). Denk hierbij aan illegale online markten en sites met beeldmateriaal van kindermisbruik. Andere cybercrime activiteiten vinden plaats door gebruik te maken van de netwerkinfrastructuur (botnets/DDoS aanvallen/Trojaanse paarden)

- **Twee beleidsstrategieën ter voorkoming en vermindering van cybercrime**

-> **Dark web indexing:**

-> het identificeren van dark websites

-> goede strategie tegen dark web websites/applicaties

-> minder effect op ransomware

-> nog het minste effect op identiteitsdiefstal / datalekken of DDoS aanvallen

-> dus vooral effectief ter voorkoming van cybercrime wat gepleegd wordt bovenop het netwerk

-> **ISP Botnet Mitigation:**

-> ISP's nemen contact op met gebruikers wanneer PC is geïnfecteerd en denken mee aan een oplossing

-> proberen SPAM-mail te signaleren en in je ongewenste e-mail te steken

-> veel effect op ransomware aanvallen en DDoS aanvallen

-> ISP botnet mitigation is dus vooral effectief ter voorkoming van cybercrime die gebruik maakt van de netwerkstructuur van het internet