OPDRACHT WORKSHOP 1 DE WERELD VAN CYBERCRIME

1) KIES 2 RECENTE DREIGINGSBEELD-RAPPORTEN (NL + INTERNATIONAAL)

Nederlands (overheid): **NCTV – *Cybersecuritybeeld Nederland 2025 (CSBN 2025)*
Kern: dreigingen worden diverser en onvoorspelbaarder; mix van statelijke actoren, cybercriminelen, afhankelijkheden, AI, telecomsector en basishygiëne.

Internationaal: **Verizon – *2025 Data Breach Investigations Report (DBIR) Executive Summary*
Kern: wereldwijde data over incidenten/breaches, aanvalsvectoren (credentials + kwetsbaarheden), sectorverschillen, motieven (financieel/spionage) en supply-chain/third-party factor.

2) ANALYSE – DE BELANGRIJKSTE DREIGINGEN

1. **Misbruik van kwetsbaarheden (vooral "edge devices"/VPN/firewalls) als instappunt**
    - **DBIR**: exploitatie van kwetsbaarheden als initial access groeit en komt rond **20%**; edge/VPN-targeting stijgt sterk.
    - **CSBN**: edge devices blijven "onverminderd aantrekkelijk"; voorbeeld met kwetsbaarheid bij systemen die tot noodprocessen leidde.
2. **Credential abuse + social engineering (phishing/impersonation)**
    - **DBIR**: credential abuse blijft de meest voorkomende vector; daarnaast veel social engineering-patronen.
    - **CSBN**: generatieve AI maakt o.a. social engineering sneller, overtuigender en schaalbaarder (teksten, audio/video).
3. **Ransomware en "system intrusion**
    - **CSBN** noemt ransomware-incidenten met grote impact en datadiefstal (zorg/lab).
    - **DBIR** noemt ransomware als blijvende grote dreiging, o.a. in overheid.
4. **Keten-/leveranciersrisico (third-party)**
    - **DBIR** benadrukt de rol van third-party relaties als terugkerend thema.
    - **CSBN** noemt incidenten bij toeleveranciers/dienstverleners die doorwerken als datalekken bij afnemers.
5. **DDoS en beschikbaarheidsverstoring**
    - **DBIR:** Denial of Service (DoS/DDoS) is een veelvoorkomend incident-patroon dat vooral de beschikbaarheid raakt (diensten worden traag/onbereikbaar), maar het leidt meestal niet tot een bevestigd datalek (breach).
    - **CSBN:** meerdere DDoS-aanvallen zorgden voor tijdelijke uitval van diensten, zoals problemen met inloggen.

3) BEANTWOORD DE VIER VERPLICHTE VRAGEN (A–D)

A) WELKE ORGANISATIES WORDEN HET MEEST GETROFFEN EN WAAROM?

Kort antwoord: bijna iedereen, maar vooral organisaties met (1) veel data, (2) vitale/ketenafhankelijke processen, (3) groot aanvalsoppervlak en/of (4) lage basishygiëne.

Concreet (met voorbeelden uit de rapporten):

- **Overheid & publieke diensten:** aantrekkelijk door maatschappelijke impact en gevoelige data; ransomware blijft een grote factor in overheden.
- **Zorg:** veel medische/persoonsdata en hoge druk → grote schade bij uitval; DBIR laat grote aantallen incidents/breaches in healthcare zien.
- **Financieel & verzekeren:** direct geld/identiteit/credentials; DBIR toont dominantie van financieel motief.
- **Telecom & digitale dienstverleners:** "hub-functie" (anderen leunen erop). CSBN noemt telecom als sector waar spionage/sabotage/PII samenkomt en waar impact snel doorrolt naar andere sectoren.
- **MKB:** vaak minder capaciteit/volwassenheid; DBIR geeft aan dat in (o.a.) retail/SMB context veel slachtoffers kleinere organisaties zijn.

B) BELANGRIJKSTE MOTIEVEN VAN CYBERCRIMINELEN (EN ANDERE ACTOREN)

- **Financieel (geld):** afpersing (ransomware), fraude, verkoop data/credentials. DBIR laat in meerdere sectoren een hoog aandeel "financial motive" zien.
- **Spionage (informatiepositie):** vooral statelijke actoren; CSBN beschrijft diversiteit aan statelijke activiteit en geopolitieke dynamiek.
- **Sabotage/ontwrichting:** CSBN benoemt dat incidenten kunnen doorwerken naar het fysieke domein en processen kunnen verstoren.
- **Ideologisch / geopolitiek gedreven hacktivisme:** CSBN noemt DDoS-campagnes en vermenging/steunstructuren rondom actoren in geopolitieke context.

C) HOE BEÏNVLOEDEN DEZE DREIGINGEN DE OPERATIONELE ACTIVITEITEN?

Denk in **CIA + continuïteit**:

- **Beschikbaarheid:** DDoS of ransomware → systemen (tijdelijk) onbruikbaar; CSBN noemt uitval/ontkoppelen van systemen en werken via noodprocessen met impact op dagelijkse werkzaamheden en ketens.
- **Integriteit:** manipulatie van data of systemen → verkeerde beslissingen, fraude, onbetrouwbare dossiers.
- **Vertrouwelijkheid:** datalekken (patiëntdata, persoonsgegevens, bedrijfsgeheimen) → juridische gevolgen, reputatieschade, afpersing.
- **Ketenimpact:** leverancier geraakt → jouw organisatie ook geraakt (doorwerking).
- **Herstelkosten en stilstand:** patchen/forensics/herstel + omzetverlies + productiviteitsverlies.

D) TRENDS/PATRONEN IN DOELWITTEN EN AANVALSMETHODEN

- **“Complexer en onvoorspelbaarder” dreigingslandschap** (mix van actoren + geopolitiek + afhankelijkheden).
- **Edge devices/VPN als snelweg naar binnen** (kwetsbaarheid-exploitatie neemt toe).
- **Third-party/supply chain als multiplier** (één leverancier → veel slachtoffers).
- **Generatieve AI versterkt bestaande dreigingen** (sneller scannen, overtuigender phishing/impersonation, hulp bij malware).
- **“Basishygiëne blijft de barrière”**: CSBN zegt letterlijk dat veel incidenten ontstaan doordat basishygiëne niet op orde is; basisprincipes werken nog steeds tegen een groot deel van de aanvallen.