1 Cybercrime Unit

1.1 Inleiding tot Cybercrime

Definitie en Relevantie

- **Cybercrime**: Misdaad gepleegd met of gericht op informatiesystemen.
- **Groeiende Probleem**: Anonimiteit, laagdrempeligheid, financieel lucratief, globalisering, gebrek aan bewustzijn, en Cybercrime-as-a-Service (CaaS).

Actuele Context

- **Trends**: Toename phishing, ransomware, en AI-gerelateerde aanvallen (bijv. deepfakes).
- **Impact**: Belgische slachtoffers verloren €40 miljoen aan phishing in 2023; ransomware-aanvallen stegen met 176% in 2023.

1.2 Cybercrime Fundamentals

Malware

- **Definitie**: Schadelijke software (spyware, ransomware, Trojaanse paarden, cryptojackers).
- **Soorten**:
  - **Worm**: Verspreidt zich via zelfkopiëring.
  - **Ransomware**: Blokkeert toegang tot data tot losgeld betaald wordt.
  - **Rootkits**: Externe toegang tot systemen.

Hacking

- **Typen Hackers**:
  - **White Hat**: Ethisch hacken voor beveiligingsverbetering.
  - **Black Hat**: Kwaadwillige exploitatie van kwetsbaarheden.
  - **Grey Hat**: Infiltreert systemen zonder toestemming, maar zonder schade.
- **Belgische Wetgeving**: Alle hacking is strafbaar tenzij vooraf toegestaan door organisatie.

Phishing

- **Definitie**: Misleidende berichten om gevoelige informatie te stelen.
- **Vormen**: E-mail, SMS, social media, voice cloning.
- **Herkenning**: Dringende taal, onverwachte verzoeken, slechte grammatica.

Ransomware

- **Proces**: Verkenning → Inbraak → Data-exfiltratie → Afpersing.
- **Trends**: Focus op datadiefstal i.p.v. alleen blokkering; gebruik van zero-day kwetsbaarheden.

1.3 Digitale Bewijsvoering en Onderzoek

Proces

Acquisitie: Verzamelen van digitale gegevens (apparaten, netwerkdata). **Analyse**: Onderzoek van bestanden, metadata, en transacties. **Chain of Custody**: Documentatie van bewijsketen om authenticiteit te garanderen.

Uitdagingen

- **Mobiele Forensics**: Encryptie, cloudopslag, diversiteit in hardware/software.
- **IoT Forensics**: Smart devices (bijv. slimme horloges, beveiligingscamera's) als bron van bewijs.

Casestudy: SKY ECC

- **Resultaten**: 48 arrestaties, >500 dossiers, 1 miljard berichten onderschept (2021–2023).

1.4 Ontwikkelingen en Trends

AI in Cybercrime

- **Aanvallen**: Automatisering van phishing, malwarecreatie met tools zoals ChatGPT.
- **Deepfakes**: Misbruik voor identiteitsfraude en desinformatie.
- **Verdediging**: AI voor malware-detectie en netwerkanalyse.

IoT Risico's

- **Kwetsbaarheden**: Default credentials, botnets (bijv. Mirai), ransomware op slimme apparaten.
- **Impact**: Manipulatie van industriële systemen (bijv. Stuxnet, 2010).

Data Explosie

- **Volume**: 120 zettabytes gegenereerd in 2023; 60% van internetverkeer via mobiel.

1.5 Veilig Online

Basisprincipes

- **Technisch**: Up-to-date antivirus, regelmatige backups, encryptie.
- **Gedrag**: Gezonde scepsis (geen verdachte links klikken), privacy-instellingen optimaliseren.

Paswoordbeheer

- **Regels**: Lange wachtwoorden met speciale tekens; gebruik van password managers.
- **Tools**: Offline managers zoals KeePass.

Data Privacy

- **Risico's**: Data brokers verzamelen persoonlijke informatie (adres, inkomen, gezondheidsdata).
- **Preventie**: Meld datalekken via CERT.be of Safeonweb.

Key Points to Remember

- **Cybercrime-definitie**: Misdaad via of gericht op informatiesystemen.
- **Phishing**: Meest voorkomende vorm; herkenbaar aan dringende taal.
- **Ransomware Flow**: Verkenning → Inbraak → Afpersing.
- **Ethisch Hacken**: Strafbaar in België zonder toestemming.
- **IoT Risico's**: Default credentials en botnets zijn grootste bedreigingen.
- **AI Dual Use**: Zowel tool voor aanval (deepfakes) als verdediging (malware-detectie).
- **Preventie**: Up-to-date software, sterke wachtwoorden, bewustzijn van sociale engineering.