Threat Landscape and Good Practice Guide for Internet Infrastructure

Threat Mind Map

- **Threats**
  - **Physical attacks**
    - Bomb attacks/threats
    - Frauds
    - Sabotage
      - Divers manipulated sea cable in Egypt
    - Vandalisms
    - Thefts
      - Devices
      - Storage media
      - Cables
      - Documents
    - Information leakages/sharing
    - Unauthorised physical access/unauthorised entry to premises
    - Coercions, extortions or corruptions
    - Briberies/corruptions
  - **Outages**
    - Lack of resources
      - Lack of human resources
      - Lack of processing power
      - Lack of network capacities
      - Lack of storage capabilities
      - Lack of physical resources
        - Power
        - Water
        - Cooling
    - Fuel exhaustions
    - Loss of power
      - Power cut
    - Power surges
    - Absence of personnel
    - Strikes
    - Loss of support services
    - Cooling outages
    - Network outages
  - **Nefarious activity/Abuse**
    - Identity theft (identity fraud/account or service-session hijacking)
    - Unsolicited e-mail
    - Malware and viruses
      - Viruses
      - Worms
      - Trojans
      - Rootkits
      - Botnets
      - Spyware
      - Scareware
      - Rogueware
    - Potentially unwanted software
      - Adware
      - Greyware
    - Abuse of information leakages
    - Compromising confidential information (data breaches)
    - Generation and use of rogue certificates
      - SSL CA infiltration
        - DigiNotar
      - Improperly issued SSL certificates
        - National Informatics Center (India)
    - Manipulation of hardware and software
    - Manipulation of information
      - Falsification of records
      - Routing table manipulations
        - Address space hijacking (IP prefixes)
      - DNS manipulations
        - DNS spoofing
          - DNS poisoning
      - Falsification of configurations
      - AS manipulation
        - AS hijacking
    - Misuse of information/information systems
    - Abuse of authorizations
    - Abuse of personal data
    - Unauthorised activities
      - Unauthorised use of administration of devices and systems
      - Unauthorised access to information systems/networks
        - IMPI Protocol
        - DNS Registrar Hijacking
      - Unauthorised changes of records
      - Unauthorised installation of software
      - Unauthorised use of software
    - Denial of service attacks (DoS/DDoS)
      - Volume
        - Amplification/reflection
          - NTP
          - DNS
          - SNMP
          - NetBios
          - SSDP
          - CharGen
          - QOTD
          - BitTorrent
          - Kad
          - Steam
          - Quake Network Protocol
          - ZAv2
        - Spoofing
        - Flooding
          - UDP
          - ICMP (Ping)
          - Slowloris
      - Applications
        - Ping of Death
        - XDoS
        - WinNuke
      - Protocol exploitations
        - TCP-SYN
        - Push+Ack
      - Malformed packet attacks
        - IP address options
    - Timescales
      - Large scale scans/probes
      - Targeted attacks/advanced persistent threats
    - Social engineering
      - Pretexting/hoax
      - Phishing
        - Spear phishing
        - Whaling
        - Baiting
    - Intended similarity of identifiers
      - Domain name collision
      - Typosquatting
    - Remote activities (execution)
    - Exploitation of software bugs
      - Kernel flaws
      - Design flaws
      - Buffer overflows
      - Race conditions
    - Validation
      - Input
        - SQL injections
        - Cross site scripting (XSS)
      - Authentication
        - Cross site request forgery
    - Brute force
  - **Disasters**
    - Natural disasters
      - Earthquakes
      - Floods
      - Tsunamis
      - Landslides
      - Lightning strike
      - Heavy rains
      - Heavy snowfalls
      - Heavy winds
      - Wildfire
      - Electromagnetic storm
    - Environmental disasters
      - Fires
      - Dangerours radiation leaks
      - Pollutions
      - Dusts
      - Corrosions
      - Unfavourable climatic conditions
      - Major events in the environment
      - Explosions
  - **Failures/Malfunctions**
    - Failures of parts of devices
      - Linecards
      - Connectors
    - Failures of devices or systems
      - Network devices
      - Servers
      - Data centers
    - Failures or disruptions of communication links (communication networks)
      - Cable breaks
      - Cable cuts
    - Failures or disruptions of main supply
      - Power
      - Cooling
      - Water
    - Failures of disruptions of service providers (supply chain)
    - Failures or disruptions of the power supply
    - Malfunctions of parts of devices
      - Linecards
      - Connectors
    - Malfunctions of devices or systems
      - Network devices
      - Servers
      - Data centers
    - Software bugs
    - Configuration errors
      - Misconfigurations
  - **Unintentional damages (accidental)**
    - Information leakage/sharing
    - Erroneous use or administration of devices and systems
    - Using information from unreliable sources
    - Unintentional changes of data in an information systems
    - Inadequate designs and planning or lack of adaptions
      - Inadequate specifications
      - Inadequate usability
      - Insecure interfaces (APIs)
      - Policy/procedure flaws
      - Design errors
  - **Damage/Loss (IT assets)**
    - Damage caused by a third party
      - Internal cases
      - External cases
        - Ship collides with cable
    - Damages resulting from penetration testing
    - Loss of information
    - Loss of (integrity of) sensitive information
    - Loss of reputation
      - Sybil attacks
      - Unfair ratings
      - Playbooks
      - Discriminations
      - Collusions
      - Proliferation
      - Reputation lag exploitations
      - Re-entries
      - Value imbalance exploitations
    - Loss
      - Devices
      - Storage media
      - Cables
      - Documents
    - Destruction of records, devices or storage media
    - Power surges
    - Wildlife
      - Rats
      - Sharks
      - Mice
  - **Eavesdropping/Interception/Hijacking**
    - Interception compromising emissions
    - Interception of information
      - Espionage
        - Nation state espionage
        - Corporate espionage
      - Rogue hardware
      - Software interceptions
    - Interfering radiations
    - Replay of messages
    - Man in the middle/session hijacking
      - Route leaks
      - BGP sessions
      - Network injection
    - Repudiation of actions
  - **Legal**
    - Violation of laws or regulations/breach of legislation
    - Judiciary decisions/court orders
      - No-IP Microsoft domains seizure
    - Failure to meet contractual requirements

https://t.me/learningnets