Resursa informațională afectată: Datele personale stocate în infrastructurile IT ale organizațiilor.

Modus operandi al amenințării: O amenințare majoră actuală identificată de ENISA este utilizarea vulnerabilităților zero-day în atacurile cybernetic. Acestea sunt exploatări care vizează vulnerabilități necunoscute anterior în software și hardware, ceea ce face ca soluțiile de securitate să fie ineficiente până când vulnerabilitatea este descoperită și remediată. În lumea bunurilor digitale piratate (software, filme, muzică…), o versiune piratată este calificată drept „Zero-Day" atunci când este disponibilă în același timp sau înainte de lansarea oficială. Literal, versiunea pirat este publicată la zero zile după lansarea publică.

Actori amenințări: Hackeri individuali și grupuri de hacker, statele naționale implicate în spionaj cibernetic și sabotaj, hacktiviști: care efectuează atacuri pentru a promova anumite ideologii politice sau sociale, organizații criminale care se concentrează pe atacuri cibernetice organizate pentru profit.

Măsuri de protecție aferente: Având în vedere natura lor, nu există o protecție 100% posibilă împotriva tuturor exploatărilor Zero-Day. Protecția va veni dintr-un set de măsuri împreună cu o echipă de securitate vigilentă:

- Monitorizarea anomaliilor, cum ar fi blocările sistemului sau modificările performanței, poate descoperi încercări de exploatare;
- Segmentarea internă a rețelei ajută la atenuarea propagării, permițând doar traficul între sistemele care trebuie conectate;
- Software-ul de atenuare a exploatărilor, cum ar fi EMET de la Microsoft, poate împiedica funcționarea anumitor exploatări.