TOP 10 kibernetičkih prijetnji do 2030. godine

1 Kompromitacija lanca opskrbe zbog ovisnosti softvera

Sve veća integracija komponenti i sustava trećih strana može dovesti do nepredviđenih ranjivosti i kompromitacije lanca opskrbe.

2 Napredne kampanje dezinformiranja

Razvoj Deepfake tehnologije predstavlja opasnost za razne oblike manipulacije.

3 Porast autoritarnosti digitalnog nadzora

Tehnologija prepoznavanja lica, nadzor interneta i baze podataka o korisnicima, potencijalna su meta kriminalnih skupina. U pitanje se dovodi i gubitak privatnosti.

4 Ljudski faktor i zastarjeli sustavi

Brz razvoj IoT-a, spora prilagodba sustava i nedostatak vještina mogu dovesti do slabijeg razumijevanja funkcioniranja kibernetičko-fizičkog ekosustava te njegove ranjivosti.

5 Napredni ciljani napadi

Korištenjem podataka prikupljenih s uređaja spojenih na internet, napadači mogu bolje prilagoditi napade ciljanom pojedincu.

6 Nedostatak analize i kontrole svemirske infrastrukture i objekata

Zbog ispreplitanja privatne i javne svemirske infrastrukture i tehnologije, potrebno je detaljno testirati njezinu sigurnost kako ne bi došlo do njezine ranjivosti.

7 Porast naprednih hibridnih prijetnji

Napadači sve češće koriste kombinaciju fizičkih i kibernetičkih napada za ostvarivanje cilja.

8 Nedostatak vještina

Organizacije s manjkom digitalnih vještina i sigurnosnih treninga su lakše mete za napadača.

9 Prekogranični pružatelji IKT usluga kao kritična točka

IKT sektor je česta meta napadača jer povezuje kritične usluge kao što su prijevoz i energetska mreža. Potrebno ga je zaštititi kako ne bi bio iskorišten kao oružje u potencijalnom sukobu.

10 Zloupotreba umjetne inteligencije

Manipulacijom algoritma umjetne inteligencije može doći do njezine zlouporabe za širenje lažnih vijesti, prikupljanje osjetljivih podataka, manipulaciju podacima i sl.

CERT.hr surfaj sigurnije

Izvor: ENISA Foresight exercise 2022

CARNET znanje povezuje