

JAK NA INTERNET

Máme se bát kybernetických útoků?

KLÍČOVÁ SLOVA

bezpečnost, CSIRT, DDoS, informační infrastruktura, kybernetický útok

OTÁZKY K DISKUZI

1. Vzpomenete si na nějaké kybernetické útoky, které se staly během posledního roku? Kdo byl napaden? Kdo byli útočníci? Co bylo cílem těchto útoků?
2. Jakým způsobem chráníte svá digitální zařízení proti kybernetickým hrozbám?
3. Proč je důležité, aby se všichni lidé připojení k internetu snažili zajistit vlastní online bezpečnost?
4. Který zákon řeší legislativní stránku počítačové bezpečnosti v České republice?
5. Jaké úkoly má „Národní centrum kybernetické bezpečnosti“?
6. Čemu se věnují bezpečnostní týmy označené jako CSIRT?
7. Slyšeli jste o projektu FENIX? Jaký je jeho účel v případě kybernetických útoků?
8. Jaké mohou být důvody, že někdo začne vést kybernetický útok?
9. Kdo jsou lidé, kteří kybernetické útoky páchají?
10. Co znamená zkratka DDoS? Co je principem tohoto typu útoku?

ÚKOLY

- A) Vyberte si nějaké noviny, ať už tištěné nebo digitální, a zjistěte, jestli za poslední rok psali o nějakých kybernetických útocích. Udělejte krátký přehled zjištěných faktů o těchto útocích.
- B) Co motivuje hackery k tomu, že se například snaží prolomit do cizího systému nebo ukrást citlivá data? O možných motivech diskutujte.
- C) Vyhledejte znění Zákona č. 18/2014 Sb. o kybernetické bezpečnosti a vyhledejte informace o stavu kybernetického nebezpečí. Zjistěte tamtéž, jaké povinnosti má vládní CERT tým.

