Typy útokov na IT

Pracovný list

Zapojenie

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Úloha 1** | Priraďte typy škodlivých programov k ich popisom. Pracujte v skupinách. Svoj výber zdôvodnite.   |  |  |  | | --- | --- | --- | | ***Typy malvéru*** |  | ***Popis*** | | *MitMO (Man-In-the-Mobile)* |  | 1. *Malvér vytvorený na automatické spúšťanie akcií obvykle online* | | *Vírus* |  | 1. *Malvér vytvorený na zablokovanie počítačového systému alebo dát, ktorý obsahuje výzvu na zaplatenie* | | *Trojský kôň* |  | 1. *Malvér určený na modifikovanie OS za účelom vytvorenia zadných vrátok (backdoor)* | | *Ransomware* |  | 1. *Malvér, ktorý sa často sa viaže na legitímny softvér, tento malvér je určený na sledovanie aktivity používateľa* | | *Bot* |  | 1. *Škodlivý spustiteľný kód, ktorý je priložený k iným spustiteľným súborom, často sú to legálne programy* | | *Scareware* |  | 1. *Malvér, ktorý robí škodlivé operácie pod pláštikom nejakých normálnych požadovaných operácií* | | *Adware* |  | 1. *Malvér niekedy zviazaný s iným softvérom a je určený na automatické spúšťanie reklám* | | *Červ* |  | 1. *Malvér na prevzatie kontroly nad mobilným zariadením* | | *Spyware* |  | 1. *Malvér, ktorý je určený na presvedčenie používateľa, aby urobil určitú akciu na základe jeho strašenia, strachu* | | *MitM (Man-In-The-Middle)* |  | 1. *Umožňuje útočníkovi prevziať kontrolu nad zariadením bez vedomia používateľa a zachytiť informácie o používateľovi predtým, ako ho odovzdá do určeného cieľa* | | *Rootkit* |  | 1. *Škodlivý kód, ktorý sa replikuje (vytvára svoje kópie) pomocou nezávislého využívania bezpečnostných dier v počítačovej sieti* | |

Skúmanie

|  |  |
| --- | --- |
| **Úloha 2** | V prehliadači načítajte stránku <http://preventista.sk/info/spustite-siet-2-ked-sa-vam-sluzba-odoprie/> a prečítajte si úvodné dve časti venované **DoS** a **DDoS útokom**. Na základe prečítaného zodpovedzte v stručnosti nasledovné otázky:   1. Čo znamená skratka **DoS** (po anglicka, po slovensky)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2. Čo môže mať za následok útok na server? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 3. V čom sa líši útok **DDoS** od útoku **DoS**? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 4. Ako získa útočník kontrolu nad iným počítačom? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 5. Čo je to **zombie** počítač? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 6. Čo je to  **botnet**? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Rozpracovanie

|  |  |
| --- | --- |
| **Úloha 3** | Vyskúšajte si **phishingový test**  na stránke <https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html>. |

Hodnotenie

Sebahodnotiaca rubrika

|  |  |
| --- | --- |
| **Čo som sa naučil/naučila...** | |
| Uviesť niekoľko príkladov na malvér | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Vlastnými slovami vysvetliť, ako prebieha DoS a DDos útok | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Vysvetliť, čo je to phishing | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Identifikovať niektoré znaky phishingového e-mailu | **VIEM / VIEM S POMOCOU / NEVIEM** |