1. Upravte následující text tak, aby jeho znění bylo pravdivé.

Ochrana dat je přístupem bránícím přerušení zákaznických služeb, a to i v případě, kdy dochází k jejich požadované změně.

Bezpečnostní síťový systém informačně-bezpečnostní infrastruktury dané společnosti či organizace.

Bezpečnostní služby jsou realizovány jako dle zabezpečení.

Bezpečnostní podporují bezpečnostní služby a provádějí specifické činnosti zaměřené na ochranu proti potenciálním útokům.

semiinvazivní nebo invazivní útoky jsou útoky aktivními.

bezpečnostní hrozby jsou škodlivé.

1. Označte v následujícím textu pravdivá tvrzení.

□ Pojem síťová bezpečnost (*Network Security*) se týká pouze bezpečnostních opatření realizovaných v počítačích na obou koncích komunikačního řetězce.

□ Zabezpečení sítě je stejně důležité jako zabezpečení jednotlivých počítačů a zajištění šifrování přenášených zpráv.

□ Bezpečnostní síťový systém je souborem hardwarových zařízení, která využívají kryptografické algoritmy k ochraně informačních a komunikačních systémů společnosti.

□ Veškeré bezpečnostní mechanismy využívají kryptografických transformací.

**X** Bezpečnostní mechanismy lze rozdělit na ty, které jsou implementovány na určité protokolové vrstvě a ty, které nejsou spojeny s jakoukoliv konkrétní protokolovou vrstvou nebo bezpečnostní službou.

**X** Schopnosti útočníka jsou typicky určeny úrovní jeho znalostí, zda je možné odhalit případné stopy po jeho útoku a mírou vynaložených nákladů nutných pro úspěšný útok na zařízení.

1. Přiřaďte správný termín z levého sloupce odpovídajícímu popisu uvedenému v pravém sloupci.

|  |  |  |
| --- | --- | --- |
| Virus |  | Škodlivý software šířený prostřednictvím sítí. |
|  |  |  |
| Červ (*Worm*) |  | Projevuje se jako neškodný program, ale může provádět činnosti, které neměl uživatel v úmyslu a kterých si ani nemusí být vědom. |
|  |  |  |
| Trójský kůň (*Trojan*) |  | Programy instalované bez vědomí a souhlasu uživatele, které provádí analýzu jeho chování, mezi které patří např. sběr informací o činnosti a využívání prohlížečů. |
|  |  |  |
| Zombie |  | Samokopírovatelné programy, které nevyžadují pro své šíření jiné soubory. |
|  |  |  |
| Spyware |  | Samokopírovatelné programy, které využívají pro své šíření infikované soubory. |

1. Doplňte do následující tabulky čísla pravdivých tvrzení.

|  |
| --- |
| 2 |
| 4 |
| 6 |
| 7 |
|  |
|  |
|  |

**1** – Malware je závadný typ softwaru.

**2** – Pojem skener je odkazem na program, který je využíván hackery k vzdálenému určení potenciálně zranitelných míst napadaného systému.

**3** – Skenovacím typem útoku je takový útok, kdy se útočník vydává za jiné zařízení nebo uživatele v síti.

**4** – Antivirové programu mohou mít i své nevýhody, např. mohou ovlivnit svou činností výkonnost počítače (systému).

**5** – Odstraněním viru se rozumí proces odstranění škodlivého kódu v infikovaném souboru, který danému viru odpovídá.

**6** – Firewall je typickým hraničním kontrolním mechanismem, resp. perimetrem obrany.

**7** – Některé systémy IDS (*Intrusion Detection Systems*) pouze monitorují a upozorňují na potenciální útoky, zatímco jiné se mohou snažit tyto útoky i zablokovat.