

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

Ochrana dat je (~~volitelným~~) (~~nezbytným~~) (~~reakčním~~) (**aktivním**) přístupem bránícím přerušení zákaznických služeb, a to i v případě, kdy dochází k jejich požadované změně.

Bezpečnostní síťový systém (~~je globální řešení~~) (**je jen malá část**) informačně-bezpečnostní infrastruktury dané společnosti či organizace.

Bezpečnostní služby jsou realizovány jako (~~bezpečnostní algoritmy~~) (**bezpečnostní mechanismy**) dle (~~protokolů~~) (**zásad**) zabezpečení.

Bezpečnostní (~~protokoly~~) (**mechanismy**) podporují bezpečnostní služby a provádějí specifické činnosti zaměřené na ochranu proti potenciálním útokům.

(~~Ne všechny~~) (**Všechny**) semiinvazivní nebo invazivní útoky jsou útoky aktivními.

(~~Ne všechny~~) (**Všechny**) bezpečnostní hrozby jsou škodlivé.

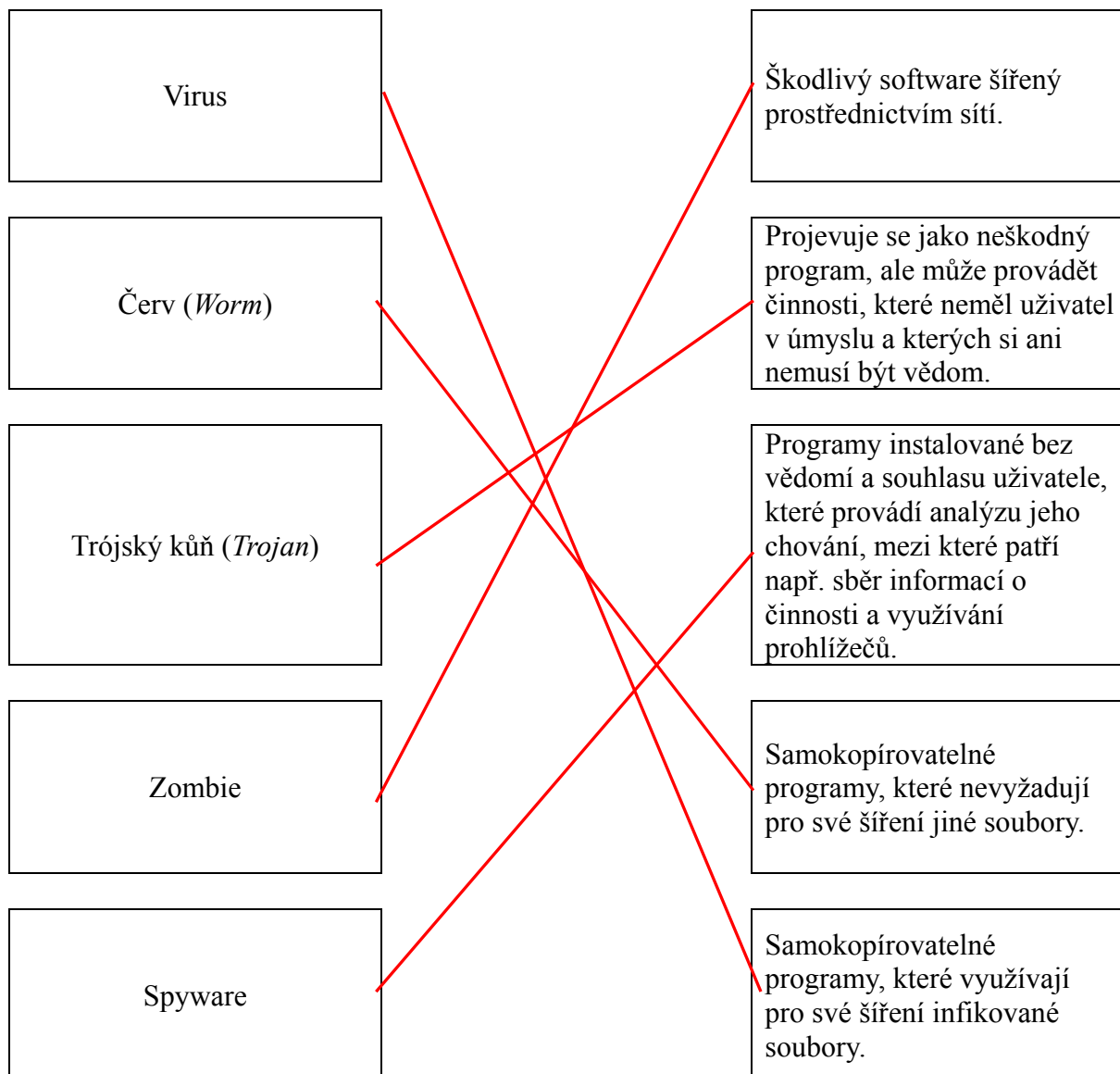


2. Označte v následujícím textu pravdivá tvrzení.

- ☐ 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.



3. Přiřad'te správný termín z levého sloupce odpovídajícímu popisu uvedenému v pravém sloupci.



4. 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.

