

**1. Wählen Sie jeweils eine Variante des folgenden Textes, so dass die Aussage richtig ist.**

Die Sicherung von Daten ist eine  $\left( \begin{array}{l} \text{wählbare} \\ \text{notwendige} \end{array} \right) \left( \begin{array}{l} \text{proaktive} \\ \text{reaktive} \end{array} \right)$  Methode zur Vermeidung einer Unterbrechung von Kundendiensten, und zwar auch während ihrer Änderung.

Das Sicherheitssystem eines Netzwerkes stellt  $\left( \begin{array}{l} \text{nur einen kleinen Teil} \\ \text{eine globale Lösung} \end{array} \right)$  der Informationssicherheitsinfrastruktur einer Firma dar.

Sicherheitsdienste werden von  $\left( \begin{array}{l} \text{Sicherheitsmechanismen} \\ \text{Sicherheitsalgorithmen} \end{array} \right)$  nach den erforderlichen  $\left( \begin{array}{l} \text{Sicherheitsprotokollen} \\ \text{Sicherheitsgrundsätzen} \end{array} \right)$  implementiert.

Die  $\left( \begin{array}{l} \text{Sicherheitsprotokolle} \\ \text{Sicherheitsmechanismen} \end{array} \right)$  unterstützen die Sicherheitsdienste und führen spezifische Aktivitäten für den Schutz vor potentiellen Angriffen durch.

$\left( \begin{array}{l} \text{Alle} \\ \text{Nicht alle} \end{array} \right)$  semi-invasiven oder invasiven Angriffe sind aktive Angriffe.

$\left( \begin{array}{l} \text{Alle} \\ \text{Nicht alle} \end{array} \right)$  Sicherheitsbedrohungen sind vorsätzlich.



**2. Markieren Sie die richtigen Aussagen.**

- Die Netzwerksicherheit betrifft nur die Sicherheit in den Rechnern, die den Anfang und das Ende der Kommunikationskette darstellen.
- Die Sicherung des Netzwerkes ist ebenso wichtig wie die Sicherung der Rechner und die Verschlüsselung von Nachrichten.
- Das Sicherheitssystem eines Netzwerkes ist ein Satz von Hardwaregeräten, die kryptographische Algorithmen zum Schutz von Informations- und Kommunikationssystemen einer Firma nutzen.
- Alle Sicherheitsmechanismen verwenden kryptographische Transformationen.
- Sicherheitsmechanismen werden in zwei Gruppen unterteilt: Mechanismen, die in einer spezifischen Protokollschicht integriert werden, und Mechanismen, die nicht mit spezifischen Protokollschichten oder Sicherheitsdiensten verbunden sind.
- Die Tauglichkeit eines Angreifers wird typischerweise von seinen Fähigkeiten, seinen hinterlassenen Spuren nach der Attacke und den erforderlichen Kosten seiner Ausstattung bestimmt.

**3. Ordnen Sie dem Begriff in der linken Spalte die entsprechende Beschreibung in der rechten Spalte zu.**

Virus	Schädliche, sich in einem Netzwerk ausbreitende Software
Wurm	Erscheint als gutartiges Programm, kann jedoch Aktionen durchführen, die vom Benutzer nicht beabsichtigt wurden oder gar nicht wahrgenommen werden
Trojaner	Software, die ohne Zustimmung des Benutzers installiert wurde und sein Verhalten verfolgt, z. B. Informationen über seine Surfgeohnheiten erfasst
Zombie	Selbstreplizierendes Programm, das keine weitere Dateien zur Verbreitung verwendet
Spyware	Selbstreplizierendes Programm, das zu seiner Verbreitung infizierte Dateien verwendet



**4. Ergänzen Sie die Nummern der richtigen Aussagen in die folgende Tabelle.**


- 1 – Malware ist eine fehlerhafte Software.
- 2 – Ein Scanner ist ein Softwareprogramm, das von Hackern zur Fern-Bestimmung von potentiellen Vulnerabilitäten eines Systems verwendet wird.
- 3 – Eine Scan-Attacke ist ein Angriff, bei der sich ein Angreifer als ein anderes Gerät oder Benutzer im Netzwerk ausgibt.
- 4 – Antivirenprogramme können auch Nachteile haben - sie können die Leistung eines Rechners beeinträchtigen.
- 5 – Die Eliminierung eines Virus bedeutet die Beseitigung des Codes in der infizierten Datei, der dem Virus entspricht.
- 6 – Eine Firewall ist typischerweise ein Mechanismus zur Grenzkontrolle oder Verteidigung am Perimeter.
- 7 – Einige IDS-Systeme dienen nur der Überwachung und warnen vor einer Attacke, wobei andere versuchen, sie zu sperren.