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

(E-Mail-Spoofing / ~~E-Mail-Sniffing~~) schließt das Senden von Nachrichten aus einer betrügerischen E-Mail-Adresse oder Fälschung der E-Mail-Adresse eines anderen Benutzers ein.

DoS-Angriffe (~~zerstören~~ / zerstören nicht) und/aber (~~stehlen~~ / stehlen nicht) Daten wie andere Angriffsarten.

Das Ziel eines (DDoS-Volumenangriffes / ~~DDoS-Protokollangriffes~~) ist die Auslastung der Bandbreite des angegriffenen Netzwerkes.

Social-Engineering-Angriffe (~~beziehen sich~~ / beziehen sich nicht) auf die technologische Manipulation der Vulnerabilitäten der Rechnerhardware oder -software und (erfordern / ~~erfordern keine~~) fortgeschrittene technische Fähigkeiten des Angreifers.

Die (~~signaturbasierte~~ / heuristische) Erkennung von Viren kann neue Viren oder Varianten der bestehenden Viren durch das Suchen von bekannten schädlichen Codes oder (geringen / ~~bedeutenden~~) Variationen dieses Codes in Dateien identifizieren.

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

2. Markieren Sie die richtigen Aussagen.

X Ein DoS-Angriff ist eine vorsätzliche Aktion, die eine Funktion eines Rechners oder Netzwerks verhindert (beispielsweise blockiert sie das Einloggen).

☐ Adware ist eine ungesetzliche Alternative für Kunden, die für Software nicht bezahlen möchten.

☐ Die Infektion mit Spyware generiert keine unerwünschte CPU-Aktivität, Plattennutzung oder Netzverkehr.

X Ein Computerprogramm, das eine Aktivität ausübt, die ein System oder Daten vorsätzlich beschädigt, wird schädlicher Code (*Malicious Code*) genannt.

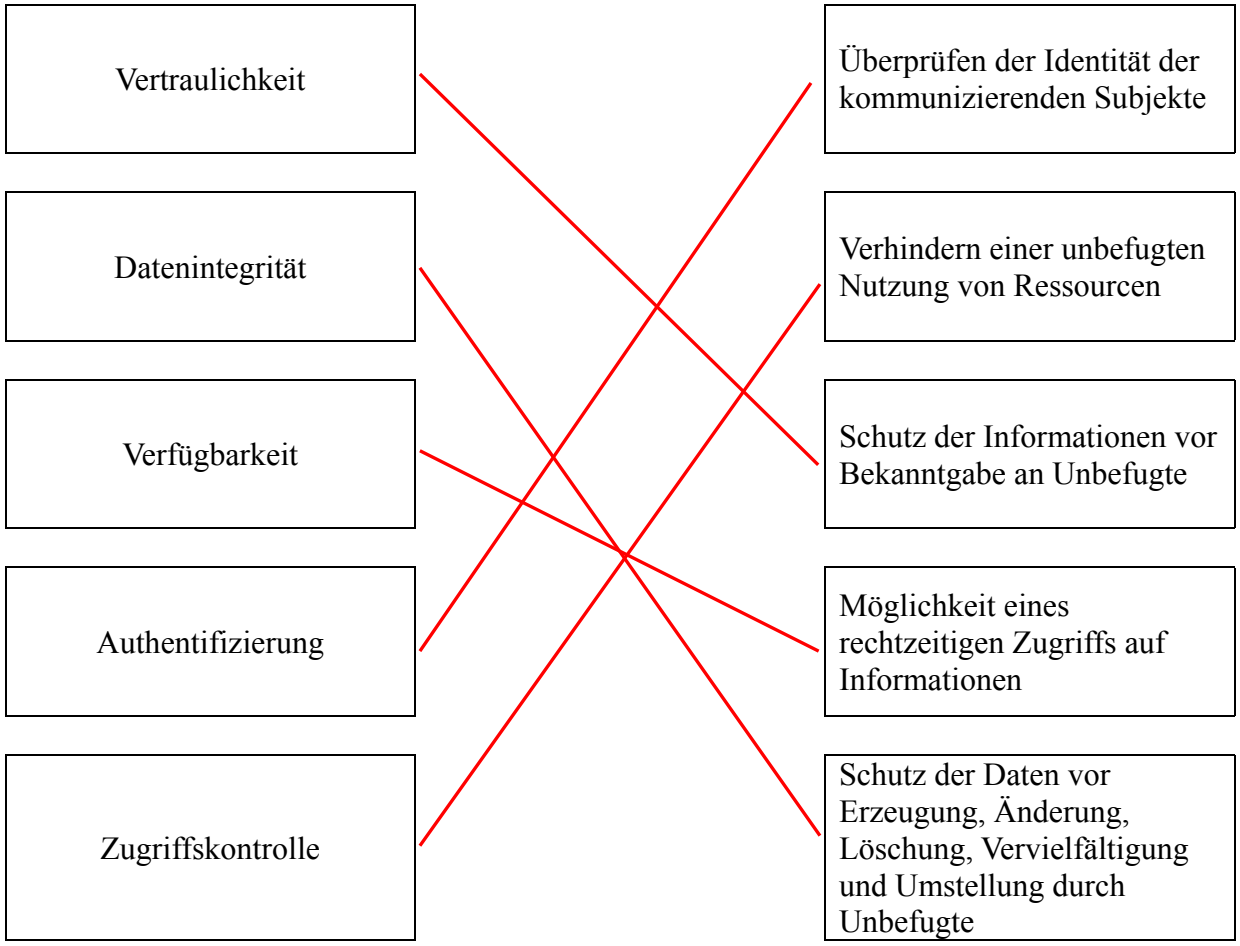
X Unter einem Spoofing-Angriff versteht man eine Handlung, bei der sich ein Angreifer als ein anderes Gerät, Benutzer oder Netzwerk ausgibt.

☐ Zero-Day-Angriffe werden in wenigen Minuten entdeckt.

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

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



Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

4. Tragen Sie die Nummern der richtigen Aussagen in die folgende Tabelle ein.

2
4
5
7

1 – Unleugbarkeit erlaubt einer Person zu kontrollieren, welche Informationen über sie erfasst werden und wie und von wem sie genutzt werden.

2 – Traffic-Padding ist ein Mechanismus, der Bits in Lücken innerhalb eines Datenflusses ergänzt, um die Verkehrsanalyse zu verhindern.

3 – Datenschutz bezieht sich auf den Schutz von Informationen vor Offenbarung Unbefugten.

4 – Beglaubigung ist ein Mechanismus, der durch einen zuverlässigen Dritten bestimmte Eigenschaften des Datentauschens gewährleistet.

5 – Eine semi-invasive Attacke kann das angegriffene Gerät manipulieren, gelangt jedoch in keinen direkten elektrischen Kontakt mit der Oberfläche des Chips.

6 – Replizieren von Knoten und Spoofing sind Beispiele passiver Attacken.

7 – Man kann ein System durch Überlauf des Puffers abstürzen lassen.

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.