Spick LB1:

- **Hoax**: Falsche Information, die sich verbreitet, oft per E-Mail oder soziale Medien, um Nutzer zu täuschen oder zu beunruhigen.

- **DMZ (Demilitarisierte Zone):** Netzwerkbereich zwischen internem Netzwerk und externem Netzwerk wie dem Internet, der zusätzlichen Sicherheit bietet, indem er potenziell gefährdete Systeme isoliert.

- **Hash**: Ein Hash ist eine Funktion, die eine Eingabe (wie eine Nachricht oder Daten) in eine feste Länge von Zeichen umwandelt. Es wird häufig verwendet, um Daten zu verschlüsseln oder zu überprüfen, ob Daten unverändert sind.

- **Ransomware**: Schadsoftware, die Daten oder Systeme verschlüsselt und Lösegeld fordert, um sie wieder freizugeben.

- **Malware**: Bösartige Software, die entwickelt wurde, um Systeme zu infiltrieren, Daten zu stehlen oder Schaden zu verursachen.

- **Exploits**: Schwachstellen oder Sicherheitslücken in Software oder Systemen, die ausgenutzt werden, um unbefugten Zugriff zu erlangen oder Schaden zu verursachen.

- **Zero Day Lücke**: Sicherheitslücke in Software oder Systemen, die den Entwicklern noch nicht bekannt ist oder für die noch kein Patch verfügbar ist.

    - Wer findet sie: Blackhat Hacker
    - Wer Nutz diese aus: Kriegsparteien, Geheimdienste, «Mafia»
    - Gegenmassnahmen: Honeypods, Blocklist, Monitoring, IDS

- **Zertifikate**: Digitale Zertifikate, die verwendet werden, um die Identität von Websites, Personen oder Organisationen zu authentifizieren und die Integrität von Daten zu gewährleisten.

Asymmetrische und Symmetrische Verschlüsselung:

- **Symmetrische** Verschlüsselung: Eine Methode, bei der sowohl die Verschlüsselung als auch die Entschlüsselung mit **demselben Schlüssel** erfolgt. Dieser Schlüssel wird sowohl vom Sender als auch vom Empfänger verwendet. Bekannte symmetrische Verschlüsselungsalgorithmen sind beispielsweise **AES** (Advanced Encryption Standard) und DES (Data Encryption Standard).

- **Asymmetrische** Verschlüsselung: Eine Methode, bei der **unterschiedliche Schlüssel** für die Verschlüsselung und die Entschlüsselung verwendet werden. Es gibt einen öffentlichen Schlüssel, der für die Verschlüsselung verwendet wird und frei verteilt werden kann, sowie einen privaten Schlüssel, der zur Entschlüsselung benötigt wird und geheim gehalten werden muss. Bekannte asymmetrische Verschlüsselungsalgorithmen sind beispielsweise **RSA** (Rivest-Shamir-Adleman) und ECC (Elliptic Curve Cryptography).

Resilienz:

IKT-Resilienz steht für Informations- und Kommunikationstechnologie-Resilienz. Es bezieht sich darauf, wie gut ein System oder eine Organisation in der Informations- und Kommunikationstechnologie auf unerwartete Störungen reagieren und sich davon erholen kann.

IDS:

IDS steht für Intrusion Detection System. Es handelt sich um eine Software- oder Hardwarelösung, die den Datenverkehr in einem Netzwerk oder auf einem Computersystem überwacht, um Anzeichen von unerlaubtem oder verdächtigem Verhalten zu erkennen und darauf zu reagieren.

IPS:

IPS steht für Intrusion Prevention System. Es ist eine Technologie, die ähnlich wie ein Intrusion Detection System (IDS) den Datenverkehr in einem Netzwerk überwacht, jedoch im Gegensatz zu einem IDS auch in der Lage ist, unerwünschte oder bösartige Aktivitäten proaktiv zu blockieren oder zu verhindern, anstatt sie nur zu erkennen und zu melden.

CIA (Confidentiality Integrity Availability)

CIA ist ein grundlegendes Konzept der Informationssicherheit und steht für Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) von Daten. Vertraulichkeit bedeutet, dass Daten nur von autorisierten Personen eingesehen werden können, Integrität bezieht sich auf die Unversehrtheit und Korrektheit der Daten, während Verfügbarkeit sicherstellt, dass Daten zu jeder Zeit für autorisierte Benutzer zugänglich sind.

Integrität, Vertraulichkeit, Verfügbarkeit:

Diese sind grundlegende Schutzziele der Informationssicherheit. Integrität bezieht sich darauf, dass Daten korrekt und unverändert bleiben; Vertraulichkeit bedeutet, dass nur autorisierte Personen auf Daten zugreifen können; Verfügbarkeit bedeutet, dass Daten und Systeme zuverlässig und rechtzeitig verfügbar sind.