ISO/IEC Standards (27001): 5 Threats

The CIA triad of cybersecurity (C=confidentiality, I=integrity, A=availability) is at the heart of a secure network environment (secure applications and secure data protection) (Kubura et al., 2020).

Moving straight forward, the **confidentiality** aspect refers in that sense to the fact that sensitive data always has a sender and one (or multiple) receiver(s) which should only be allowed to have access to the related data. The most common cause that can violate confidentiality is an attacker who already entered and monitors the network where the data flows on and therefore sits in between sender and receiver. A second problem can occur when the attacker already has sensitive data such as a username and password of a user so that he has direct access to some parts of the data without thinking about how to enter the network as a whole. How a user can avoid such a “password-hacking”? There are multiple solutions but already using strong passwords and/or changing the password more often is a starting point (Kubura et al., 2020) (Fowler, 2017).

Explaining **integrity** of data in a rough sense is relatively simple. Integrity refers to the correctness of the data that someone requests. In other words, that what you see, use or query in a digital environment should be that what it would be in a secure world. Hence, the question what an attacker could intend also comes directly to mind, accessing the data and manipulate it. How a user can protect against it? Two-Factor Authentication for example. To be more precise, someone who is authorized to CRUD operations should always be obliged to confirm that he is the person which a network expects he is (Kubura et al., 2020) (Enisa, 2021).

Availability is more a problem related to business goals. It refers to that the fact that data should always accessible for several people at the same time. The idea that an

attacker could manipulate the data in the sense of the last paragraph (integrity) is much worse than the way where the malicious user displays a “personal” message which already indicates that the system has been hacked. How to attenuate that risk? Beside Two-Factor Authentication good cipher text encryption of the data is helpful (Kubura et al., 2020) (Fowler, 2017).

A final, general advice for companies is related to cyber training. Employees should be taught how far reaching the **consequences** of an attack are and why for example **access control** is implemented. Specifically, the last point should also be dependent on the qualification and position of an employee. In other words, getting on the next level in a career should be more and more evaluated on technical know-how of an employee and cybersecurity knowledge should be a part of it (See point Perception in (pwc, 2021)).

Reference List:

ENISA (2021). *ENISA THREAT LANDSCAPE 2021 April 2020 to mid-July 2021*. [online] European Union Agency for Cybersecurity (ENISA), 2021, pp.1–116. Available from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Accessed 23 June 2022].

Fowler M. (2017) The Basics of Web Application Security. Available from: https://martinfowler.com/articles/web-security-basics.html [Accessed 24 June 2022]

Kuburat O. A. A., Khmaies O., Adnan m. Abu-Mahfouz & Suvendi R. (2020) A Surey on the Security of Low Power Wide Area Networks : Threats, Challenges, and Potential Solutions. *Sensors*, Vol 20, Iss 5800, p 5800 (2020); MDPI AG.

Pwc (2021) How CEOs can pass the cybersecurity leadership test. Available from: https://www.pwc.com/gx/en/issues/reinventing-the-future/take-on-tomorrow/cybersecurity-leadership.html [Accessed: 24. June 2022]