Collaborative Discussion 1 – Summary Post – Michael Geiger

Cyber security is a multi-dimensional subject area that has to be considered on complex levels and has to meet various demands of aspects.

While companies have to fear long-term damage to their reputation as a result of a cyber attack in addition to data loss, a cyber breach can affect the democratic system in relation to nations (Troncoso, 2019). In addition to the ethical consideration on a large scale, a cyber breach has drastic consequences for private individuals, as the theft of sensitive personal data not only encroaches on their fundamental rights, but also has direct consequences, such as the theft of financial and intellectual property or even physical hazards, as a result of publication of the place of residence(Ben-Hassine, n.d.). Therefore, Governments have a great interest in monitoring and actively defending in the event of a cyber attack by intervening in corporate systems and supporting companies in closing cyber breaches in order to maintain security (National Cyber Security Centre, n.d.). Even if systems can never be completely secure, companies for their part have the responsibility to design their cyber presence and offerings in such a way that they meet the requirements of their customers and the law, as well as that a cyber breach can be ruled out as far as possible (Mokhor et al., 2020).

To pursue this goal, the CIA triad model can be used, which addresses the three aspects of information security in a service-related system. These are confidentiality, the protection against access to private data by third parties. Integrity, the security that data is not manipulated and availability, the guarantee of continuous access to the data by authorized persons. (Chai, n.d.)

In conclusion, it can be stated that cyber security is of great importance for private individuals, companies and also nations and will become more necessary as a result of further networking and development.

References:

Ben-Hassine, W. (n.d.) Government Policy for the Internet Must Be Rights-Based and User-Centred. United Nations. Available from: https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred [Accessed 26.08.2021]

Chai, W. (n.d.) Confidentiality, integrity and availability (CIA traid). Techtarget. Available from: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA [Accessed 27.08.2021]

Mokhor, V., Honchar, S., Onyskova, A. (2020) Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects. Institute of Electrical and Electronics Engineers. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9467957 [Accessed 26.08.2021]

National Cyber Security Centre (n.d.) Introduction. Available from: https://www.ncsc.gov.uk/section/active-cyber-defence/introduction#:~:text=Active%20Cyber%20Defence%20(ACD)%20seeks [Accessed 26.08. 2021]

Troncoso, C. (2019) The Cyber Security Body of Knowledge. Available from: https://www.cybok.org/media/downloads/Privacy__Online_Rights_issue_1.0_FNULPel.pdf [Accessed 27.08.2021]