Peer Review 1 – 186650356 (The Human Factor June 2022)

Very well structured and detailed list of threats and associated requirements and expectations. Three important factors in human factor threats are identified, broken down in detail and analysed in the context of the CIA. In order to go into more depth in the presentation on factors and mitigation measures in the context of the human factor, the following questions can be reflected:

Lack of Knowledge:

- How can cyber security training be designed so that it is adapted to the individual progress and awareness developments of the users, is positively received and is intrinsically motivating (Michie et al., 2011)?
- (How) can web browser requirements and DDOS attacks be applied to human behaviour?

Knowing-doing gap:

- How can vulnerability checks be carried out in a human context so that they do not deter users (as demonstrative), but are perceived as helpful and profitable (Van’t Wout, 2019)? (Positive feedback culture)
- What password policy can be followed so that secure passwords are used and protected from unauthorized persons?

Misuse of privileges:

- How can malicious users be detected at an early stage (Maasberg et al., 2020)?
- Are there measures that reduce the risk of malicious misuse on a psychological level? (Positive work environment; Respectful & appreciative work culture; Reward mechanisms for good work / good behaviour)

References:

Maasberg, M., Van Slyke, C., Ellis, S. & Beebe, N. (2020) The dark triad and insider threats in cyber security. *Communications of the ACM*. *63*(12): 64-80. Available from: https://dl.acm.org/doi/fullHtml/10.1145/3408864 [Accessed 07 July 2022].

Michie, S., Van Stralen, M. M., & West, R. (2011) The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, *6*(1): 1-12. Available from: https://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-6-42?report=reader [Accessed 07 July 2022].

Van‘t Wout, C. (2019) Develop and maintain a cybersecurity organisational culture. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS.* 457-466. Available from: https://books.google.de/books?hl=de&lr=&id=UfedDwAAQBAJ&oi=fnd&pg=PA457&dq=Cyber+security+vulnerability+check+feedback+culture&ots=CZEH8JnNd1&sig=xDMUfRVAAA2hf8YhLgTPnlv7Jp0&redir_esc=y#v=onepage&q&f=false [Accessed 08 July 2022].

Peer Review 2 – 1864805875

The essay highlights important aspects that must be considered in order to contribute to good cyber security. Authentication and system configuration in particular are subject areas which must be examined in depth on a psychological level within the framework of human factors in order to find appropriate solutions in relation to security, usability and functionality tenet and to make the ASMIS user-friendly and secure at the same time. However, the following aspects should be considered:

Authentication

- Two-factor authentication (2FA) is one of the most secure authentication methods, but it has some disadvantages in terms of usability and functionality.
- The 2FA leads to a higher workload of the users and lower usability (Krol et al., 2015).
- A device, usually a Smartphone, is required and skills are needed for a safety usage. It has to be considered that statistically a large number of patients belong to older age cohorts and could potentially have no Smartphone or are not able to use it properly.

System configuration

- In addition to automation processes, the design can contribute to better security through user-friendly handling. Hartson and Pyla (2018) summarize good recommendations under the five types of 'Affordance'.

User awareness training

- User awareness training must be individually adapted in order to generate the greatest possible yield (Michie et al., 2011).

References:

Hartson, R., & Pyla, P. S. (2018) *The UX book: Agile UX design for a quality user experience*. Morgan Kaufmann. Available from: https://0-www-sciencedirect-com.serlib0.essex.ac.uk/book/9780128053423/the-ux-book?via=ihub= [Accessed 09 July 2022].

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015) "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. *arXiv preprint arXiv:1501.04434*. Available from: https://arxiv.org/abs/1501.04434 [Accessed 09 July 2022].

Michie, S., Van Stralen, M. M., & West, R. (2011) The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, *6*(1): 1-12. Available from: https://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-6-42?report=reader [Accessed 07 July 2022].