Individual Presentation – transcript – Michael Geiger

Hello, my name is Michael Geiger. In this presentation, I will highlight the importance of human factors in relation to cyber security and discuss which aspects should be considered when implementing an appointment and scheduling management information system (ASMIS) in order to mitigate threats of cyber breaches.

In order to actively prevent threats based on human factors, psychological concepts must first be considered so that suitable countermeasures can be developed.

Sasse and Rashid (2019) emphasize that risks of human errors arise from non-compliance users. Structures, procedures and offers must therefore be developed to design the ASMIS, making it user-friendly and secure at the same time in order to motivate them becoming compliant users.

The argument should be considered, that security is not the top priority for users. They primarily want their work to be done easily and quickly.

The Security, Functionality and Ease-of-use triangle shows that simply focusing on security implementations can lead to usability and functionality suffering, making the system less attractive to users and lead them to develop techniques to circumvent the security measures (Waite, 2010).

A balanced consideration of all three of these aspects must be made in order to design a secure but also user-friendly application, which motivates the users through the functions to use the security mechanisms and to consider them as useful.

Mental models and designing persona can help to anticipate the potential usage behaviour of users in the development process of the application (Hartson & Pyla,

2018). Psychological considerations such as human capabilities, emotional states and mood, short-term and long-term memory, as well as previous knowledge must be taken into account in order to develop appropriate security structures and to offer users individually tailored assistance to increase the security of the system.

In order to shed light on these aspects, the mitigation approaches are divided into three categories:

Security by Environment, which influences the working environment and 'sensory stimuli'.

Security by Design, the design of the ASMIS application.

And Security by Intervention, through learning and awareness programs that address the individual strengths and needs of users.

Security by Environment

Johnson (2020) shows that people have a limited attention span. The average person can store information for only 30 seconds, or up to 2 minutes with focused concentration, before it is erased from short-term memory. 4 plus or minus 1 items can be stored at the same time.

However, situations and influences can result that these human capacities being adversely affected. Noise and a hectic work environment, which are often found in a clinic, are two dominant factors that must be considered.

An appropriate working environment must therefore be created, which not only prevents physical access to the end devices for unauthorized persons and protects against information being made available through unauthorized insights, but also offers employees a pleasant working atmosphere that promotes concentration.

A spatial separation is an obvious approach. In addition, studies also show that appropriate music can have a positive influence on people. Humans can selectively focus on certain auditory stimuli and hide disruptive ones. Music can also influence the human pulse (Fukumoto & Nomura, 2009). Vanderhaegen et al. (2020) states that the heartbeat can have a crucial influence on human errors.

For example, in the field of sports songs are chosen that have specific beats per minute, since the heartbeat adapts to this rhythm. A similar approach, but with a soothing effect, can be used in the clinic to encourage the concentration of receptionists and doctors while calming the patients (Fallek et al., 2020).

Security by Design

In addition to the external factors that affect the concentration of employees, the design of the ASMIS can be chosen in such a way that processes can be carried out easily and assistance is provided when necessary. Here, simple features can make a significant contribution to usability.

Hartson and Pyla (2018) list five types of affordance that should be considered when designing to increase the usability: ‘Cognitive affordance’ , ‘Physical affordance’, ‘Sensory affordance’, ‘Functional affordance’ and ‘Emotional affordance’.

For example, intuitively understandable progress displays can be implemented. If, due to distraction or other factors, a user of the ASMIS has forgotten which section was last edited and where it needs to be continued, visual aids can provide helpful cognitive assistance.

Prior knowledge of the user should also be taken into account when creating the application. For example, many websites have the log-out function in the upper right corner. Choosing this function at the same place can make it easier for the user to use it, since they may have already had the same experience and thus transfer previous knowledge to the application. Therefore mental models and persona should be considered and created in the developing process to be able to plan different typical users and their expected behaviour.

Furthermore, the psychological influence of colours on human perception should be also taken into account in order to use them in a targeted manner. Johnson (2020) lists recommendations that should be considered when choosing colour for the design. For example it is recommended to use cream colours primarily.

Studies show that the colour green has a calming and positive mood effect on users and can also slow down the heartbeat (Elliot & Maier, 2007; Al-Ayash et al., 2016). The colour red has the opposite effect. This psychological influence can be used in a targeted manner to support functions through the design. For example, the layout of the application can be selected in a cream green to create a pleasant atmosphere. Warnings can flash in orange-yellow if necessary information has not yet been provided or the user has something to consider. Only in special cases should an intense red colour be chosen, for example when the user is about to discard or delete

something, or an IT employee is about to perform an unusual or even potentially harmful operation.

Pop-ups can provide support for these coloured signals. By popping up these notes, human attention is drawn to the information that is important at the moment and can prevent from being overlooked.

Security through Intervention

So that the users of the ASMIS know which aspects have to be considered in relation to handling access data, working at their workplace and threats such as phishing attacks, cyber security awareness trainings (CSAT) are of fundamental importance, especially in the healthcare sector (Kamerer et al., 2020).

However, making CSAT a purely periodic compulsory event for all employees is not enough to guarantee a sustainable acquisition of skills (Zhang et al., 2021).

He and Zhang (2019) indicate a number of sociological and psychological aspects that need to be considered when designing CSAT:

Employees may find the security training boring due to the design. A clumsy presentation of videos followed by a multiply-choice test is not helpful for a long-term learning effect.

Positive incentives must be created to increase motivation. An example could be a Cyber Security Reward for particularly good behaviour.

CSAT should be tailored to the individual needs and previous knowledge of the employees in order to enable an optimal learning effect and to increase interest.

Individual learning strategies should be considered and offers should be made available via various media such as texts, films or interactive games.

The CSAT should be regularly revised and adapted to be up to date. Feedback should be considered in order to increase the quality of learning.

Another recommendation is the segmentation of user types in order to be able to offer individually adapted security training. The information required for this can be collected through previous CSAT courses and also enables companies to operate customized risk management.

A general segmentation of the population in the United Kingdom for vulnerabilities to cybercrime was examined by Home Office, Research, Information and Communication Unit (2015) as shown in the figure.

With regard to companies, OutThink (2021) presents a segmentation matrix that structures users according to their knowledge of security and their feelings about security.

For example, naive users have good intentions, but do not have the knowledge to act safely. In contrast, there are shadow agents who have the knowledge but are unwilling to use it.

By this segmentation it possible to analyze skills and behaviour patterns in a targeted manner and to develop individually adapted training offers or security measures.

Conclusion:

It can be summarized that all three listed subject areas, Security by Environment, Security by Design and Security through Intervention must be reflected under the human and psychological aspects in order to optimize cyber security. When designing the work environment, attention should be paid to a good working atmosphere and sources of irritation should be minimized in order to promote the cognitive capacities and work ethic of the employees.

When choosing the design of the application, the five types of affordance and psychological aspects of the design, such as the respective colour choice, should be considered in order to prevent human error and increase usability.

Advanced training for users through cyber security awareness training should be individually tailored to needs and learning behaviour in order to motivate participants to learn safe behaviour and to create a long-term effect.

Thank you for your attention

References:

AL-Ayash, A., Kane, R. T., Smith, D., & Green-Armytage, P. (2016) The influence of color on student emotion, heart rate, and performance in learning environments. *Color Research & Application*. *41*(2): 196-205. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/col.21949 [Accessed 21 July 2022].

Elliot, A. J., & Maier, M. A. (2007) Color and psychological functioning. *Current directions in psychological science*. 16(5): 250-254. Available from: https://journals.sagepub.com/doi/full/10.1111/j.1467-8721.2007.00514.x [Accessed 15 July 2022].

Fallek, R., Corey, K., Qamar, A., Vernisie, S., Hoberman, A., Selwyn, P., Fausto, J. A., Marcus, P., Kvetan, V. & Lounsbury, D. (2020) Soothing the heart with music: A feasibility study of a bedside music therapy intervention for critically ill patients in an urban hospital setting. *Palliative and Supportive Care.* 18(1): 47-54. Available from: https://www.cambridge.org/core/journals/palliative-and-supportive-care/article/abs/soothing-the-heart-with-music-a-feasibility-study-of-a-bedside-music-therapy-intervention-for-critically-ill-patients-in-an-urban-hospital-setting/7C3B901165040FD7390A6DB113F07ECD [Accessed 13 July 2022].

Fukumoto, M., & Nomura, S. (2009) The change in the synchronization between heartbeat and music. *Journal of Medical Informatics & Technologies*. Available from: https://scholar.google.de/scholar?hl=de&as_sdt=0%2C5&q=THE+CHANGE+IN+THE+SYNCHRONIZATION+BETWEEN+HEARTBEAT+AND+MUSIC&btnG= [Accessed 13 July 2022].

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 11 July 2022].

He, W., & Zhang, Z. (2019) Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*. *29*(4): 249-257. Available from: https://www.tandfonline.com/doi/abs/10.1080/10919392.2019.1611528 [Accessed 21 July 2022].

Home Office, Resarch, Information and Communction Unit (2015) *Serious and Organised Crime Protection Public Interventions Model: Defining the Vulnerable Groups.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502960/Gov.uk_Serious_Organised_Crime_deck_vF.pdf [Accessed 22 July 2022].

Islam, S. (2020) Measuring human risk and targeting behaviour change. Digital 2020 ISF World Congress. Available from: https://www.youtube.com/watch?v=zrI6YVf4qeI&t=1278s [Accessed 20 July 2022].

Johnson, J. (2020) Designing with the mind in mind: simple guide to understanding user interface design guidelines. *Morgan Kaufmann*. Available from: https://essexonline.vitalsource.com/reader/books/9780128182031/pageid/124 [Accessed 12 July 2022].

Kamerer, J. L., & McDermott, D. (2020) Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*. 10(4): 48-53. Available from: https://reader.elsevier.com/reader/sd/pii/S2155825620300144?token=948A746154B22584D708E1334E5917543D9391C80DCD09C3B89C2B1CC3EC4DEAD419B8974923349BE7ADD530DBF38005&originRegion=eu-west-1&originCreation=20220713083113 [Accessed 16 July 2022].

OutThink (2021) Cyber Security Human Risk Management. Available from: https://outthink.io/cyber-security-human-risk-management/ [Accessed 11 July 2022].

Sasse, M. A. & Rashid, A. (2019) Human Factors Knowledge Area. Available from: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf [Accessed 11 July 2022].

Vanderhaegen, F., Wolff, M., & Mollard, R. (2020) Non-conscious errors in the control of dynamic events synchronized with heartbeats: a new challenge for human reliability study. *Safety Science*. *129*: 104814. Available from: https://www.sciencedirect.com/science/article/pii/S0925753520302113 [Accessed 14 July 2022].

Waite, A. (2010) InfoSec Triads: Security/Functionality/Ease-of-Use. Available from: https://blog.infosanity.co.uk/?p=676 [Accessed 12 July 2022].

Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021) Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*. Available from: https://www.emerald.com/insight/content/doi/10.1108/IMDS-08-2020-0462/full/html [Accessed 21 July 2022].