Seminar 1 Preparation (With E-Portfolio Components)

Seminar 1: Scrum Security review

Please carry out these activities before joining the seminar this week. Your answers will be discussed during the seminar.

Question 1

Create a 2-column multi-line table. In the left-hand column, include the software development stages of the Scrum agile life cycle approach to project management. In the right-hand column, describe the processes which you recommend are applied at each stage to ensure that secure software is produced at the end of the development. To support the preparation of your response, you can refer to the following literature:

Sharma, A. & Bawa, R. K. (2020) Identification and Integration of Security Activities for Secure Agile Development. *International Journal of Information Technology*.

Answer:See table below:

Initial Product Backlog Creation	<u>Identification, Implementation</u> Abuse cases, Design Requirements,Security Requirements, Identify Resources and Trust Boundaries, Specify Operational Environment, Automated Acceptance and Unit Tests
Product Backlog Refinement	
Sprint Planning	
Daily Scrum	<u>Implementation, Verification</u> Role Matrix, Assumption Documentation, Requirements Inspection, Risk Analyses, Risk Metrics, Static Code Analyses, Dynamic Analysis, Pair Programming
Definition of Done	<u>Definition of Done</u> Incident Response Planning,Operational Planning and Readiness, Signing the Code
Sprint Review	<u>Identification</u> Repository Improvement, Final Security Review

Blog Post: Question 2 (also e-portfolio activity)

Some say that people are the biggest risk of cyber security.

Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300-word blog post on how people can be managed to overcome cyber security attacks from the inside.

Answer: see below post

The Human Factor

Sunday, 21 August 2022, 11:26 PM

by Jurbe Jubet

Visible to participants on this course

Edited by Jurbe Jubet, Sunday, 21 August 2022, 11:31 PM

The ISO/IEC 27000:2018 prepares standards for Information Security Management Systems (ISMS). These standards are aimed at guiding institutions to effectively manage risk (ISO, 2018). The risk posed by insider threats can be managed and we have used 5 terms and references found in the ISO/IEC 27000:2018 to show how people can be managed to overcome Cyber security attacks from the inside

The human factor plays a major role in information security. According to a study by IBM, 95% of corporate security incidences are caused by Human error (The Hacker News, 2021). In another data collected by Black Hat 2017 in Las Vegas, as reported by coresecurity, Humans are the Biggest Risk for Security breaches with an estimated 35% due to Remembering and changing passwords, 21% due to Never-ending software updates to protect against hacks, 15% due to Living under constant Cybersecurity threats and 29% due to Information overload (www.coresecurity.com., n.d.). Insider threats present another dangerous concern to information security and as report has it that internal sources are responsible for 43% of enterprise data loss (McAfee, 2015)

Access control: Access control is perhaps the most common method of managing risk posed by humans. Just as the name implies, access of users is controlled by setting permissions. A combination of user credentials is required to grant access to specific resources. There is a menace of Users stealing credentials of other users to carry out attacks, but this can also be controlled by User education, Second Factor Authentication, permission control and Behavioural Analytics (Parkin, 2020)

Audit: Auditing plays a role in identifying security failures otherwise not detected by real time countermeasures when it comes to human factor. Internal Audits while checking the effectiveness of existing controls can also identify certain risky User behaviours.

Non-repudiation: Non-repudiation is the assurance that security risk event that has occurred cannot be disputed. This poses a great risk when it comes to insider threats since the insider who knows the system very well may be able to cover the track. Transitional Non-Repudiation is used such that every transaction is connected to a specific account and that account is linked to a human that is verifiable (Fulton, 2022). This way, Users become accountable for every action they take

Outsourcing: Although organisations would like to outsource certain I.T functions to allow them focus on core functions, it is important to note that insider threats go beyond employees within the organisation to include these third parties. Outsourcing will therefore, increase the likelihood of Insider threats since the employees of the third parties may not be directly controlled

by the Outsourcing company. Insider threat controls such as Behavorial Analytics may also not be effectively carried out for the same reason. It is therefore necessary to carry out risk analysis capturing risk posed by Human errors before certain functions are Outsourced

Risk Management: An effective Insider threat management will require both proactive and reactive countermeasures (www.ekransystem.com., 2021). Preventing Insider risk event from happening can be done by enforcing Risk Management Policies such as disabling USB ports and secondary storage systems on all computers. A reactive Risk Management approach is to set up a timely and effective Incidence respond plan.

References

INTERNATIONAL STANDARD ISO/IEC 27000. (2018). [online] Available at: https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf. [Accessed 20 August 2022]

The Hacker News, (2021). Why Human Error is #1 Cyber Security Threat to Businesses in 2021. [online] Available at: https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html. [Accessed 20 August 2022]

www.coresecurity.com. (n.d.). The Biggest Risk for Security Breaches: Humans! [online] Available at: https://www.coresecurity.com/blog/biggest-risk-security-breaches-humans [Accessed 21 Aug. 2022].

McAfee, (2015) Grand Theft Data. [online] Available at: http://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf [Accessed 21 Aug. 2022].

Parkin, M. (2020). Using Access Controls to Thwart Insider Threats. [online] Security Boulevard. Available at: https://securityboulevard.com/2020/09/using-access-controls-to-thwart-insider-threats/ [Accessed 21 Aug. 2022].

Fulton, J (2022). Cybersecurity from the inside out — Guarding against insider threats | Security Magazine. [online] Available at: https://www.securitymagazine.com/articles/97919-cybersecurity-from-the-inside-out-guarding-against-insider-threats [Accessed 21 Aug. 2022].

www.ekransystem.com. (2021). What Is an Insider Threat? Definition, Types, and Countermeasures. [online] Available at: https://www.ekransystem.com/en/blog/insider-threat-definition.