Unit 2 Seminar Preparation

Question 1:

|  |  |
| --- | --- |
| Scrum Stage | How to increase security |
| Initiation | * Educate stakeholders and developers on security concepts, types of security breaches and how to mitigate security risks * Hire security experts. |
| Planning and estimation | * Add S-Tags to user stories in the backlog * Use OWASP ASVS to create security stories * Assign security related tasks to developers * Create threat model * Perform risk analysis * Change definition of done to include security requirements being met * Create detailed UML diagrams * Define project and security requirements * Add acceptance criteria to user stories * Create role matrix * Identify resources and trust boundaries * Spring planning |
| Implementation | * Perform static code analysis * Perform pen testing, automation testing, unit testing, acceptance testing, security testing, black box testing and white box testing * Pair programming * Use code linters * Use security code libraries * Run vulnerability scans * Code reviews * Apply encryption algorithms to data * Utilise design patterns * Perform quality gate checks |
| Reviewing | * Do external review * Review security policies and procedures * Monitor security metrics * Sprint Retrospectives * Daily standup |
| Releasing | * Perform code signing * Final security review * Patch any security vulnerabilities * Create incident response plan |

Question 2:

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.

How people can be managed to overcome cyber security attacks from the inside?

**How people can be managed to overcome cyber security attacks from the inside?**

As Thomas Reid rather eloquently put it “a chain is no stronger than its weakest link” (Reid, 1786). Contextualising this in terms of security the weakest link refers to the human element involved. In this blog post I am going to discuss how people can be managed to overcome cyber security attacks from the inside referencing chapter 3 from the ISO/IEC Standard.

The terms I focused on were access control, competence, monitoring, policy, and risk assessment. My rational for selecting these key terms was that I believe they play a significant role in how people can be managed to overcome cyber security attacks.

Training from leading security experts on how to spot and mitigate the latest security threats as well as educating employees on ethics, social engineering, phishing attacks, regulations, and compliance will greatly reduce the likelihood of threats to the system.

Requiring employees to take personality tests would allow organisations to spot people who could become security threats. For example, spotting vulnerable people who could be coerced. There are numerous studies done on this such as the technical report on Identifying At-Risk Employees (U.S. Department of Energy, 2010) and the journal article on Behavioural Analysis of Insider Threats (Azaria et all., 2014).

Having security policies in place, utilising security and monitoring software, having robust access controls and requiring admin approval to perform certain functions in conjunction with following the principle of least privilege help to ensure the security of a system.

As human error is one of the leading causes of cyber-attacks, I believe it’s vital for an organisation to create an atmosphere where people can learn from their mistakes. This is perfectly summed up by Henry Ford who stated, “The only real mistake is the one from which we learn nothing”.

As humans are the biggest threat to cyber security it is important that they feel valued as If a disgruntled employee could become a security threat.

**References**

*ISO/IEC 27000:2018(EN) - international organization for standardization*. ISO. Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en> [Accessed 21 March 2024]

U.S. Department of Energy (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats*. Available from: <https://doi.org/10.2172/1000159> [Accessed 21 March 2024]

Azaria, A., Richardson, S K & Subrahmanian, V S. (2014) Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data. *IEEE Transactions on Computational Social Systems* 1(22): 135-155. doi: 10.1109/TCSS.2014.2377811. [Accessed 21 March 2024]

Reid, T. (1786). Essays on the Intellectual Powers of Man. Great Britain: John Bell