Module 4 Topic 3

Worksheet

Group (or Individual) Activities

(Task 1) Consider the NCSC Security Architecture Anti-Patterns Whitepaper

https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

a. What is NCSC?

The **National Cyber Security Centre (NCSC)** is a UK government organisation providing advice and support for the public and private sectors to avoid computer security threats. It is part of the Government Communications Headquarters (GCHQ) and works to make the UK the safest place to live and work online.

b. What is Security Architecture Anti-Patterns?

Security Architecture Anti-Patterns are standard design patterns in computer systems that are ineffective and can lead to security vulnerabilities. These anti-patterns are repeated solutions to common problems that do not work and should be avoided

c. What is a whitepaper?

A **whitepaper** is an authoritative report or guide that concisely informs readers about a complex issue and presents the issuing body's philosophy. It is meant to help readers understand an issue, solve a problem, or decide.

d. What are bastion hosts?

A **bastion host** is a special-purpose computer on a network designed and configured to withstand attacks. It is used to provide access to a private network from an external network, such as the Internet, and is typically placed in a demilitarised zone (DMZ) to provide an additional layer of security

e) For each anti-pattern presented, assign it to the most relevant CIS control(s):

https://www.cisecurity.org/controls/cis-controls-list

1. Anti-pattern 1: ‘Browse-up’ for administration
   The relevant CIS controls are:

   - **CIS Control 5: Account Management** - Ensuring proper management of administrative accounts.
   - **CIS Control 6: Access Control Management** - Managing and restricting access to administrative functions

2. Anti-pattern 2: Management bypass
   The relevant CIS controls are:

   - **CIS Control 5: Account Management** - Properly managing and monitoring administrative accounts.
   - **CIS Control 6: Access Control Management** - Ensuring that access controls are enforced and not bypasse

3. Anti-pattern 3: Back-to-back firewalls
   The relevant CIS controls are:

   - **CIS Control 4: Secure Configuration of Enterprise Assets and Software** - Ensuring firewalls are properly configured.
   - **CIS Control 7: Continuous Vulnerability Management** - Regularly assessing and managing vulnerabilities in firewall configurations

4. Anti-pattern 4: Building an ‘on-prem’ solution in the cloud
   The relevant CIS controls are:

   - **CIS Control 3: Data Protection** - Ensuring data is protected in cloud environments.
   - **CIS Control 13: Network Monitoring and Defense** - Monitoring and defending cloud network configurations

5. Anti-pattern 5: Uncontrolled and unobserved third-party access
   The relevant CIS controls are:

   - **CIS Control 15: Service Provider Management** - Managing and monitoring third-party service providers.
   - **CIS Control 6: Access Control Management** - Ensuring third-party access is controlled and monitored

6. Anti-pattern 6: The un-patchable system
   The relevant CIS controls are:

   - **CIS Control 7: Continuous Vulnerability Management** - Regularly assessing and managing vulnerabilities.
   - **CIS Control 4: Secure Configuration of Enterprise Assets and Software** - Ensuring systems are configured securely and can be patched

TASK 2 – Cyber Security Discussion

You can use the following sources, or any other reputable sources, to select a data breach that you find interesting and discuss what could be done to prevent it from happening:

a. https://www.codecademy.com/article/case-studies-notable-breaches
b. https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them
c. https://www.british-assessment.co.uk/the-worst-data-breaches-in-history/

Yahoo Data Breach (2013)

Impact: 3 billion accounts

Details: In August 2013, Yahoo experienced one of the most significant data breaches in history, affecting 3 billion user accounts. The breach was not publicly disclosed until December 2016, during Yahoo's acquisition by Verizon. The attackers accessed account information, including security questions and answers, but not plaintext passwords, payment card data, or bank information

Prevention Measures:

1. **Enhanced Encryption:** Implementing stronger encryption methods for sensitive data, such as security questions and answers, could have reduced the breach's impact.
2. **Regular Security Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the system.
3. **Multi-Factor Authentication (MFA):** Encouraging or requiring users to enable MFA to add an extra layer of security to their accounts.
4. **Timely Disclosure:** Promptly disclosing breaches to affected users and regulatory bodies to mitigate potential damage and maintain transparency.
5. **Improved Monitoring:** Implementing advanced monitoring tools to detect unusual activity and potential breaches in real time.

Other Notable Data Breaches

• **Aadhaar Data Breach (2018):** Exposed the personal details of over 1.1 billion Indian citizens

• **First American Financial Corporation (2019):** Exposed 885 million sensitive records, including bank account details and Social Security numbers

• **Equifax Data Breach (2017):** Exposed the personal information of 147 million people, including Social Security numbers and credit card details

• **Marriott International (2018):** Exposed the personal information of approximately 500 million guests

Task 3 – Using scholarly papers to inform your discussion

Utilising scholarly papers as your primary source of information ensures credibility and depth in your research. Unlike blogs and casual online articles, academic papers undergo rigorous peer review processes, ensuring the content is true, reliable, and relevant to the field. By referencing such sources, you elevate the quality of your presentation and demonstrate a commitment to academic rigour and integrity, making your arguments more persuasive and your stance more authoritative. Choose academic sources to give your audience the best, most trustworthy information. For Level 5, you are expected to gain familiarity
with scholarly sources.

Consider the following two papers:

"The Challenges of Leveraging Threat Intelligence to Stop Data Breaches"

https://www.frontiersin.org/articles/10.3389/fcomp.2020.00036/full
and

"Enterprise data breach: causes, challenges, prevention, and future directions"

https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1211

Split the work between group members and then discuss your results at the end:

- *In your group, ask one person to list the significant benefits and limitations of using threat intelligence to stop data breaches.*

Paper: "The Challenges of Leveraging Threat Intelligence to Stop Data Breaches"

Benefits:

1. **Enhanced Visibility:** Provides greater visibility into potential threats, helping organisations understand their unique threat landscape
2. **Proactive Defence:** Enables proactive defence measures by identifying and mitigating threats before they can cause harm
3. **Informed Decision-Making:** Helps in making informed security decisions based on evidence-based insights
4. **Customization:** Can be tailored to the specific needs and risks of an organisation

Limitations:

1. **Complexity:** Implementing threat intelligence can be complex and requires significant resources
2. **Data Overload:** The sheer volume of threat data can be overwhelming and difficult to manage
3. **Integration Challenges:** Integrating threat intelligence with existing security systems can be challenging
4. **False Positives:** There is a risk of false positives, which can lead to unnecessary actions and resource wastage

- *Ask the second person to write a 200-word summary of each paper highlighting the future directions of the research.*

Paper 1: "The Challenges of Leveraging Threat Intelligence to Stop Data Breaches" This paper discusses the increasing importance of threat intelligence in preventing data breaches. It highlights the challenges organisations face in implementing practical threat intelligence, such as data overload, integration issues, and the need for customisation. The paper emphasises the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing threat intelligence capabilities. Future research directions include developing more sophisticated AI and ML algorithms to improve threat detection and response, as well as creating standardised frameworks for threat intelligence implementation

Paper 2: "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions" This paper reviews the causes and challenges of enterprise data breaches, including internal and external threats. It discusses various prevention and detection techniques, such as encryption, access controls, and employee training. The paper identifies future research opportunities, including developing more advanced data leak detection systems, improved incident response strategies, and integrating threat intelligence with other security measures. The authors also call for more collaboration between academia and industry to address the evolving threat landscape

- *Ask the third person to design an infographic that illustrates the principal causes AND preventative measures associated with enterprise data breaches.*

- **Main Causes of Enterprise Data Breaches:**
    - Phishing attacks
    - Insider threats
    - Weak passwords
    - Unpatched vulnerabilities
    - Misconfigured systems

- **Preventative Measures:**
    - Implementing multi-factor authentication (MFA)
    - Regular security training for employees
    - Conducting regular security audits and vulnerability assessments
    - Ensuring timely patching of software and systems
    - Using strong encryption for sensitive data