Topic 5 Discussion 3

Choose one of the following principles of cybersecurity:

* Encapsulation
* Modularity
* Simplicity of Design (Economy of Mechanism)
* Minimization of Implementation (Least Common Mechanism)
* Open Design
* Complete Mediation
* Least Privilege
* Fail-Safe Defaults/Fail-Secure
* Least Astonishment (Psychological Acceptability)
* Minimize Trust Surface (Reluctance to Trust)
* Usability
* Trust Relationships

Imagine you are the department head for a local business and your director has asked you to explain in simplistic terms the core concepts of the selected principle. Provide a clear and precise definition and example of the concept, addressing how it is used in your systems for the organization where you work.

Your cohort replies in this discussion forum should take the role of a different department head at a different location. In your cohort reply, you should explore a different principle and provide an example to build upon the cohort post and more clearly explain the concept to your director.

As the head of the IT Department, I will focus on the principle of Least Privilege.

**Definition**

Least privilege in cybersecurity is a security principle that limits user access to only the resources they need to perform their job(NIST, n.d.). This means that users should only have access to the data, applications, and systems that are absolutely necessary for their work.

**Example**

Least privilege is like giving each person only the keys to the rooms they need to do their job. For example, the kitchen staff only needs keys to the kitchen, not the storage room. The boss only needs keys to their office and the storage room, not the kitchen(Paloalto, 2024). An example would be that our sales team only has access to the customer database, not the financial records. This way, even if someone on the sales team tries to access financial information, they won't be able to.

**Usage in Our System**

In our systems, we use least privilege by giving each employee access to only the programs and files they need to do their job. This helps us keep our data safe and prevents unauthorized access.

**Cohort Response**

As the head of Software Development Department, we will put our focus into the Open Design Principle.

**Definition**

Open design in is a principle that states that the security of a system should not rely on the secrecy of its design or implementation(OWASP Developer Guide, n.d.). This means that the design and code should be open to scrutiny and review, allowing for better security analysis and identification of potential vulnerabilities.

**Example**

An example would be on our point-of-sale systems they will have open-source software. This means anyone can see the code, find potential problems, and suggest improvements. It's like having a team of security experts working for us, making our systems stronger. Open design isn't about giving away our secrets, it’s about being transparent and collaborative, making our systems more secure for everyone(Boersma, 2020).

References:

Boersma, E. (2020, October 17). *7 Application Security Principles You Need to Know | Cprime Blogs*. Cprime. https://www.cprime.com/resources/blog/security-by-design-7-principles-you-need-to-know/

National Institute of Standards and Technology. (n.d.). *least privilege - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/least\_privilege

*OWASP Developer Guide | Principles of Security | OWASP Foundation*. (n.d.). Owasp.org. https://owasp.org/www-project-developer-guide/draft/foundations/security\_principles/

Paloalto. (2024). *What Is the Principle of Least Privilege?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege