MODULE 3: FOUNDATIONAL CONCEPTS IN SECURITY
WEEK 3

Learning Outcomes:

After completing this course you are expected to demonstrate the following:

1. Classify the concept of trust, trustworthiness and ethics

A. Engage

Trivia

1. Access control systems were first developed in the 1960s as a means of dealing with the issue of lost keys. Early systems used simple key pads.
2. Where a high level of security is required, two-factor authentication can be included in 2 methods of authentication such as a code plus third party approval via video
3. Mandatory access control is mostly use by the government because of high and granular level of security
4. The Mandatory access control and Discretionary access control can combine to balance both weakness and strength.

B. Explore

Video Titles:

1. **What is Responsible Disclosure?**
2. **Data handling, Accountability, Responsibility**

YouTube Links:

1. https://www.youtube.com/watch?v=t5UKO4jjevw
2. https://www.youtube.com/watch?v=mgbCYELAGKI

Video Module Filenames:

1. **Week 3 - What is Responsible Disclosure**
2. **Week 3 - Data handling, Accountability, Responsibility**

C. Explain

Professional Ethics are principles that govern the behaviour of a person or group in a business environment. Like values, professional ethics provide rules on how a person should act towards other people and institutions in such an environment.

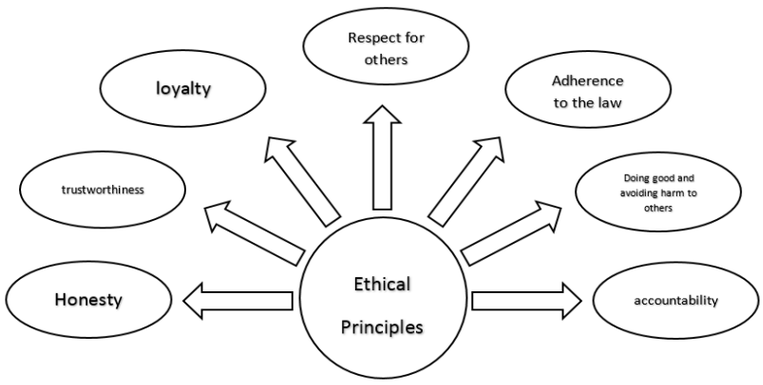

Figure 3.0
Ethical Principles

Ethical Principles

Ethical principles underpin all professional codes of conduct. Ethical principles may differ depending on the profession; for example, professional ethics that relate to medical practitioners will differ from those that relate to lawyers or real estate agents.

However, there are some universal ethical principles that apply across all professions, including:

1. Honesty
2. Trustworthiness
3. Loyalty
4. Respect for others
5. Adherence to the law
6. Doing good and avoiding harm to others
7. Accountability

D. Elaborate

Ethics (Responsible Disclosure)

Vulnerability Disclosure is an important process to keep our systems safe. What if the disclosure itself is also vulnerable?

Further, it is the process of bringing information about flaws in operating systems, applications, firmware and business processes into the public domain. The purpose is to ensure that product vendors fix the flaws while users can mitigate against them before those same flaws are also found and exploited by bad guys.

The vulnerabilities are usually discovered by security researchers who specifically look for them. Since cyber criminals and adversarial nation states are also looking for them -- and there is no way of knowing whether they have also found them -- it is essential that they are fixed as soon as they are discovered and before they are exploited. Vulnerability disclosure by good guys is an essential part of this process.

We need to understand three terms: vulnerabilities (a flaw or bug in code); exploits (a methodology used to manipulate the vulnerability); and patching (fixing the vulnerability by the vendor and implementing the fix by the user).

Zero-Day vulnerabilities

It is useful to understand the concept of zero-days (0-days). 0-day vulnerabilities are known to a potential attacker, but not yet known, and therefore not yet fixed, by the vendor. In consequence, there is in theory no defense against a 0-day exploit developed for 0-day vulnerability.

Technically, the term applies to the period between discovery and fix. This is a variable time depending on how long it takes the vendor to fix the problem. In practical terms, however, the vulnerability remains 0-day vulnerability for individuals until the vendor's fix is implemented on the user's computer.

Disclosure

Vulnerability disclosure is an important process in keeping our products secure. Security researchers find the flaws; report them to the vendors, who then fix them. That's the theory. When it works, it works well; but it doesn't always work.

Two basic approaches to vulnerability disclosure

1. **Full Disclosure**
    a. The concept of ***full disclosure*** implies the immediate and full publication of all the details of the discovered vulnerability – possibly including an exploit to demonstrate the vulnerability. Followers of this doctrine believe it is the only way to ensure the vendor fixes the problem with all possible haste.

    b. Fixing code flaws can be a time-consuming and costly exercise for the vendor, and acknowledging that they have sold software with bugs can damage their reputation. Historically, many companies have taken the view that the fewer people who know about the weakness, the more secure their product remains (and, of course, it saves them time, money and reputation). So, they do nothing, or do it very slowly.

2. **Responsible Disclosure**
    a. It is the route preferred by almost all vendors and security firms. In its raw form, this is simply the private disclosure of the vulnerability to the vendor alone, with no public disclosure until after the vulnerability has been fixed – if ever.

    b. In most cases the researcher applies a time limit. If the vulnerability isn't fixed within a certain time, it will be disclosed publicly. In practical terms, responsible disclosure is a compromise between what the vendors would like (no public disclosure) and full disclosure. Bug bounty programs have emerged where vendors offer programs that entice researchers to responsibly disclose bugs in return for compensation and recognition. These programs are somewhat controversial and warrant further discussion in the future.

Figure 3.1
Differences between known and unknown vulnerabilities

Ethics In An Information Society

Ethics is a concern of humans who have freedom of choice.

Basic Concepts: Responsibility, Accountability, and Liability

Responsibility is a key element of ethical action. ***Responsibility*** means that you accept the potential costs, duties, and obligations for the decisions you make.

Accountability is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action.

Liability extends the concept of responsibility further to the area of laws. ***Liability*** is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations.

Due process is a related feature of law-governed societies and is a process in which laws are known and understood and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

E. Evaluate

ASSESSMENT:
Instructions: You may write your answer on the Answer Sheet (AS) provided in this module.

CONTENT FOR ASSESSMENT:
For 2-points each.

1. It is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mended.
2. A feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations.
3. The practice of publishing information related to a security vulnerability found in software.
4. It means that you accept the potential costs, duties, and obligations for the decisions you make.
5. A feature of systems and social institutions

Activity No. 1:
Instructions: Answer the following questons using the Activity Sheet (ACTS) provided in this module. To be passed in next meeting.

To DOs:
1. What are the principles of secure design?
2. What is least privilege?
3. Differentiate least privilege from isolation under the principle of secure design topic.

References:

1. *https://www.caldersecurity.co.uk/40-security-facts-access-control/*
2. *https://www.synopsys.com/blogs/software-security/responsible-vulnerability-disclosure-best-practices/(image)*
3. *https://www.iaa.govt.nz/for-advisers/adviser-tools/ethics-toolkit/professional-ethics-and-codes-of-conduct*
4. *https://blog.avast.com/the-importance-of-vulnerability-disclosure-avast*
5. *https://www.osisoft.com/ethical-disclosure-policy/*
6. *https://paginas.fe.up.pt/~acbrito/laudon/ch5/chpt5-2main.htm*

Facilitated By:		
Name	:	
MS Teams Account (email)	:	
Smart Phone Number	:	