Unit 3: Best Practices for Securing Systems

Content Area: **Business**
Course(s): **Generic Course**
Time Period: **Semester 1**
Length: **4 weeks**
Status: **Published**

Enduring Understandings

Cybersecurity risk is a measure of the potential damage or loss a vulnerability could cause weighed against the likelihood an adversary will exploit the vulnerability.

The more you restrict access, processes, resources, and users based on the policy, the more secure the system.

Standards

CAEP.9.2.12.C.3	Identify transferable career skills and design alternate career plans.
CAEP.9.2.12.C.7	Examine the professional, legal, and ethical responsibilities for both employers and employees in the global workplace.
TECH.8.1.12	Educational Technology: All students will use digital tools to access, manage, evaluate, and synthesize information in order to solve problems individually and collaborate and to create and communicate knowledge.
TECH.8.1.12.A	Technology Operations and Concepts: Students demonstrate a sound understanding of technology concepts, systems and operations.
TECH.8.1.12.B	Creativity and Innovation: Students demonstrate creative thinking, construct knowledge and develop innovative products and process using technology.
TECH.8.1.12.C	Communication and Collaboration: Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others.
TECH.8.1.12.D	Digital Citizenship: Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
TECH.8.1.12.E	Research and Information Fluency: Students apply digital tools to gather, evaluate, and use information.
TECH.8.1.12.F	Critical thinking, problem solving, and decision making: Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources.
TECH.8.2.12	Technology Education, Engineering, Design, and Computational Thinking - Programming: All students will develop an understanding of the nature and impact of technology, engineering, technological design, computational thinking and the designed world as they relate to the individual, global society, and the environment.
TECH.8.2.12.A	The Nature of Technology: Creativity and Innovation: Technology systems impact every aspect of the world in which we live.
TECH.8.2.12.B	Technology and Society: Knowledge and understanding of human, cultural and society values are fundamental when designing technology systems and products in the global society.
TECH.8.2.12.C	Design: The design process is a systematic approach to solving problems.

TECH.8.2.12.D	Abilities for a Technological World: The designed world is the product of a design process that provides the means to convert resources into products and systems.
TECH.8.2.12.E	Computational Thinking: Programming: Computational thinking builds and enhances problem solving, allowing students to move beyond using knowledge to creating knowledge.

Essential Questions

- What policies and procedures are in place to keep data safe?
- How does a hardware vulnerability differ from a software vulnerability?
- What are some methods used by adversaries exploiting hardware?
- What is the Meltdown vulnerability and how many computers does it affect?
- How do hardware vulnerabilities sometimes involve software?
- How can physical security help protect potentially vulnerable hardware?
- Why are CVE and OWASP beneficial to the security community?
- What is an injection attack? What does it do?
- How can buffer overflow attacks be prevented?
- Is cryptography, regardless of what kind, a guaranteed way to secure data?
- What is the SSDLC and how does it differ from old software development methods?
- What is the difference between static and dynamic analysis?
- What are zero-day attacks and why are they so devastating?
- Are zero-day attacks always discovered by adversaries?
- Why is patching so important?

Knowledge and Skills

After completing this unit, student can:

- Define securing systems in relationship to attack vectors
- Examine methods for establishing security policies and procedures including use of benchmarks
- Identify the characteristics of vulnerability assessment
- Examine how the Common Vulnerability and Exposure database can be used as a research tool
- Identify host-based defensive tools to harden and restrict access
- Apply a vulnerability assessment tool and use results to secure a system
- Apply host-based defensive tools to secure user access and backups
- Mitigate risk of third-party applications
- Understand Threat Modeling to determine what risk you are willing to take and what effort you are willing to put in to secure your IOT devices
- Examine vulnerabilities of home Internet of Things (IOT) – examples: robot vacuum, video doorbell, smart refrigerator, voice-activated virtual assistant, etc.

Transfer Goals

Students will apply knowledge of cybersecurity concepts to engage in discussions of current events.

Students will practice digital citizenship which is an important part of 21st century culture.

Students will understand that complex mathematical models are used to keep data secure.

Students will be able to use ethical reflection and judgment regarding benefits and harms to make decisions.

Students will be able to think critically to evaluate the trust and credibility of organizations.

Students will know the importance of keeping their data secure and private.

Students will install computer updates as soon as they become available.

Students will develop a security mindset which is the ability to identify what might go wrong.

Students will be able to keep themselves and their data safe.

Resources

Curriculum is based on theGarden State Cybersecurity Curriculum