- Filename: eccouncil-ceh31250-v10-1-3-5-intro_to_ethical_hacking_security_controls_pt5.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Security Controls Pt.5
- Description: In this episode, Daniel and Zach conclude their look at Security Controls and Procedures by discussing the concept and implementation of Access Controls. Here Access Control will be defined along with its major components. You'll also learn about different Access Control mechanisms. They then move on to Data Security with topics like Data leakage and leak prevention tactics as well as Data Loss Prevention and Backup/Recovery strategies.

==========

Intro to Ethical Hacking: Security Controls Pt.5

- Access Control
    - Terminology
        - Subject
            - User or process that requests access to a resource
        - Object
            - Files, Folders, and/or Hardware that Subjects request access to
        - Reference Monitor
            - Used to check access control rules
        - Operation
            - The actual action done by Subjects and/or Objects
    - Types
        - Discretionary Access Control
            - Access rights are in the hands of users
        - Mandatory Access Control
            - Rights are dictated from on high
        - Role-based Access
            - Access based on job roles
            - Helps to quickly apply access to new users
    - Access Control Mechanisms
        - Identification
            - A method of distinguishing one account from another
                - Usernames
            - The account holder presents the ID as verification of their ID
        - Authentication
            - System for verifying the presented ID
                - Passwords
        - Authorization
            - Implemented access control based on the account holder's assigned rights
                - i.e. Read and Execute, but no Write
        - Accounting

        - Tracking system that monitors account activities
            - i.e. User1 attempted Write to file1.txt on Sept 23, 2018 01:22:42AM
    - IAM (Identity and Access Management)
        - Create, control, maintain, track, report, and remove digital identities
        - Can be used to manage
            - Employees
            - Customers
            - SSO

- Data Security
    - Unauthorized disclosure
        - aka Data Leak
        - Can be done digitally or physically
            - Digitally
                - Malicious text, email, hyper-link
            - Physically
                - Stolen devices/drives
                - Site compromise
        - Possible risks due to unauthorized disclosure
            - Loss of X
            - Legal issues
        - Threats
            - External
                - Impersonation
                    - Stolen/guessed user creds used to access data
                - Web application attacks
                - Malware
                - Phishing
            - Internal
                - Disgruntled employee
                - Blackmailed employee
                - Negligent employee
    - Data Loss Prevention(DLP)
        - The classification and monitoring of critical or sensitive data
        - Actively prevents unauthorized disclosure by way of creating and enforcing policies and procedures
            - Force encryption
            - Deny/Block access
            - Redaction (content-aware DLP)
    - Backups
        - A good backup strategy must be designed and implemented
    - Recovery
        - Recover accidentally or maliciously deleted or modified data
        - From backup
            - Good idea to test backup recovery strategy