Cyber Resilience and Redundancy

Objective 3.4: Explain the importance of resilience and recovery in security architecture

- **Cyber Resilience and Redundancy**
  - *Cyber Resilience*
    - Ability to deliver outcomes despite adverse cyber events
  - *Redundancy*
    - Having additional systems or processes for continued functionality
  - Significance of Cyber Resilience
    - Swift Recovery
      - Enables organizations to recover swiftly after cyber events
    - Continuous Operations
      - Ensures continuous operations despite attacks or technical failures
  - High Availability
    - Importance
      - Critical for continuous operations
    - Elements
      - Load balancing
      - Clustering
      - Redundancy in power
      - Connections
      - Servers
      - Services
      - Multi-cloud systems

- Data Redundancy
  - Achieved by
    - Redundant storage devices
  - Types
    - RAID configurations
- Capacity Planning
  - Importance
    - Efficient scaling during peak demand
  - Considerations
    - People
    - Technology
    - Infrastructure
- Power Components
  - Generators, UPS, line conditioners, power distribution centers (PDCs)
  - Ensures constant power supply to data centers
- Data Backups
  - Types
    - Onsite
    - Offsite
  - Methods
    - Encryption
    - Snapshots
    - Recovery
    - Replication
    - Journaling

- Business Continuity and Disaster Recovery (BC/DR) Plan
  - Importance
    - Ensures smooth business operations during unforeseen events
- Backup Site Options
  - Hot
  - Cold
  - Warm Sites
  - Geographic Dispersion
  - Virtual Sites
  - Platform Diversity
- Testing Methods
  - Tabletop Exercises
  - Failover Techniques
  - Simulation
  - Parallel Processing
  - Use Cases
    - Support different scenarios within organizations

- **High Availability**
  - High Availability Basics
    - *High Availability*
      - Aims to keep services continuously available by minimizing downtime
      - Achieved through load balancing, clustering, redundancy, and multi-cloud strategies

- Uptime and Availability Standards
  - *Uptime*
    - The time a system remains online, typically expressed as a percentage
  - *Five nines*
    - Refers to 99.999% uptime, allowing only about 5 minutes of downtime per year
  - *Six nines*
    - Refers to 99.9999% uptime, allows just 31 seconds of downtime per year
- *Load Balancing*
  - Distributes workloads across multiple resources
  - Optimizes resource use, throughput, and response time
  - Prevents overloading of any single resource
  - Incoming requests are directed to capable servers
- *Clustering*
  - Uses multiple computers, storage devices, and network connections as a single system
  - Provides high availability, reliability, and scalability
  - Ensures continuity of service even in case of hardware failure
  - Can be combined with load balancing for robust solutions
- *Redundancy*
  - Involves duplicating critical components to increase system reliability
  - Redundancy can be implemented by adding multiple
    - Power supplies
    - Network connections
    - Servers
    - Software services

        - Service providers
    - Prevents single points of failure in systems
    - Examples
        - Redundant power supplies
        - Network connections
        - Backup servers
- *Multi-Cloud Approach*
    - Distributes data, applications, and services across multiple cloud providers
    - Mitigates the risk of a single point of failure
    - Offers flexibility for cost optimization
    - Aids in avoiding vendor lock-in
    - Requires proper data management, unified threat management, and consistent policy enforcement for security and compliance
- *Strategic Planning*
    - Design a robust system architecture to achieve high availability
    - Utilize load balancing, clustering, redundancy, and multi-cloud approaches
    - Proactive measures reduce the risk of service disruptions and downtime costs
    - Safeguard organizational continuity and reliability in a competitive environment

- **Data Redundancy**
    - RAID Overview
        - *RAID (Redundant Array of Independent Disks)*
            - Combines multiple physical storage devices into a single logical storage device recognized by the operating system
    - *RAID 0*
        - Provides data striping across multiple disks

- Used for improved performance but offers no data redundancy
- Multiple drives increase read and write speeds
- Suitable for scenarios where performance is essential, and data redundancy is not a concern

- *RAID 1*
  - Provides redundancy by mirroring data identically on two storage devices
  - Ensures data integrity and availability
  - Suitable for critical applications and maintains a complete copy of data on both devices
  - Only one storage device can fail without data loss or downtime
- *RAID 5*
  - Utilizes striping with parity across at least three storage devices
  - Offers fault tolerance by distributing data and parity
  - Can continue operations if one storage device fails
  - Data reconstruction is possible but results in slower access speeds
- *RAID 6*
  - Similar to RAID 5 but includes double parity data
  - Requires at least four storage devices
  - Can withstand the failure of two storage devices without data loss
- *RAID 10*
  - Combines RAID 1 (mirroring) and RAID 0 (striping)
  - Offers high performance, fault tolerance, and data redundancy
  - Requires an even number of storage devices, with a minimum of four
- RAID Resilience Categories
  - *Failure-resistant*
    - Resists hardware malfunctions through redundancy (e.g., RAID 1)

- *Fault-tolerant*
  - Allows continued operation and quick data rebuild in case of failure (e.g., RAID 1, RAID 5, RAID 6, RAID 10)
- *Disaster-tolerant*
  - Safeguards against catastrophic events by maintaining data in independent zones (e.g., RAID 1, RAID 10)

- RAIDs are essential for ensuring data redundancy, availability, and performance in enterprise networks
- The choice of RAID type depends on specific requirements for performance and fault tolerance

- **Capacity Planning**
  - *Capacity Planning*
    - Critical strategic planning effort for organizations
    - Ensures an organization is prepared to meet future demands in a cost-effective manner
  - Four Main Aspects of Capacity Planning
    - People
      - Analyze current personnel skills and capacity
      - Forecast future personnel needs for hiring, training, or downsizing
      - Ensure the right number of people with the right skills for strategic objectives
      - Example
        - Hiring seasonal employees for holiday retail demand
    - Technology
      - Assess current technology resources and their usage

- Predict future technology demands
- Consider scalability and potential investments in new technology
- Example
    - Ensuring an e-commerce platform can handle traffic spikes

■ Infrastructure

- Plan for physical spaces and utilities to support operations
- Includes office spaces, data centers, and more
- Optimize space and power consumption
- Example
    - Data center capacity planning for server installations

■ Processes

- Optimize business processes for varying demand levels
- Streamline workflows, improve efficiency, and consider outsourcing
- Example
    - Automating employee onboarding to handle high demand

- **Powering Data Centers**
    - Key Terms
        - *Surges*
            - Sudden, small increases in voltage beyond the standard level (e.g., 120V in the US)
        - *Spikes*
            - Short-lived voltage increases, often caused by short circuits, tripped breakers, or lightning

- *Sags*
  - Brief decreases in voltage, usually not severe enough to cause system shutdown
- *Undervoltage Events (Brownouts)*
  - Prolonged reduction in voltage, leading to system shutdown
- *Power Loss Events (Blackouts)*
  - Complete loss of power for a period, potentially causing data loss and damage

- Power Protection Components
  - *Line Conditioners*
    - Stabilize voltage supply and filter out fluctuations
    - Mitigate surges, sags, and undervoltage events
    - Prevent unexpected system behavior and hardware degradation
    - Unsuitable for significant undervoltage events or complete power failures
  - *Uninterruptible Power Supplies (UPS)*
    - Provide emergency power during power source failures
    - Offer line conditioning functions
    - Include battery backup to maintain power during short-duration failures
    - Typically supply 15 to 60 minutes of power during a complete power failure
  - *Generators*
    - Convert mechanical energy into electrical energy for use in an external circuit through the process of electromagnetic induction
    - Backup generators supply power during power grid outages
    - Smaller generators for limited applications (e.g., emergency lighting)
    - Different Types of Generators

        - Portable gas-engine generators
        - Permanently installed generators
        - Battery-inverter generators
    - *Power Distribution Centers (PDC)*
        - Central hub for power reception and distribution
        - Includes circuit protection, monitoring, and load balancing
        - Integrates with UPS and backup generators for seamless transitions during power events
- Considerations for Data Centers
    - Large data centers use rack-mounted UPS for server protection
    - UPS provides line conditioning and battery backup for 10-15 minutes
    - Power distribution units manage load balancing and line conditioning
    - Backup generators are crucial for extended power outages but require startup time
    - Building data centers with redundancy and protections tailored to use cases and budgets

- **Data Backups**
    - *Data Backup*
        - Creating duplicate copies of digital information to protect against data loss, corruption, or unavailability
        - Safeguards data from accidental deletion or system failures
    - Onsite and Offsite Backups
        - *Onsite Backup*
            - Storing data copies in the same location as the original data

- *Offsite Backup*
  - Storing data copies in a geographically separate location
- Importance
  - Onsite backups are convenient but vulnerable to disasters
  - Offsite backups protect against physical disasters

- Backup Frequency
  - Determining factor of backup frequency is the organization's RPO
    - *Recovery Point Objective (RPO)*
      - Ensures that the backup plan will maintain the amount of data required to keep any data loss under the organization's RPO threshold
  - Considerations
    - Data change rate
    - Resource allocation
    - Organizational needs
- *Encryption*
  - Fundamental safeguard that protects the backup data from unauthorized access and potential breaches
    - *Data-at-rest Encryption*
      - Encrypting data as it is written to storage
    - *Data-in-transit Encryption*
      - Protecting data during transmission
    - Importance
      - Safeguarding backup data from unauthorized access and breaches
- *Snapshots*
  - Point-in-time copies capturing a consistent state

- Records only changes since the previous snapshot, reducing storage requirements
- Use cases
  - Valuable for systems where data consistency is critical, like databases and file servers

- Data Recovery
  - Several key steps in the data recovery process
    - Selection of the right backup
    - Initiating the recovery process
    - Data validation
    - Testing and validation
    - Documentation and reporting
    - Notification
  - Importance
    - Regaining access to data in case of loss or system failure; a well-defined and tested recovery plan is essential
- *Replication*
  - Real-time or near-real-time data copying to maintain data continuity
  - Benefits
    - Ensures seamless data continuity
    - Suitable for high-availability environments
- *Journaling*
  - Maintaining a detailed record of data changes over time
  - Benefits
    - Enables granular data recovery
    - Maintains an audit trail

        - Ensures data integrity and compliance
    - Considerations
        - Data tracking granularity, size, retention policies, and security

- **Continuity of Operations Plan**
    - *Continuity of Operations Plan (COOP)*
        - Ensures an organization's ability to recover from disruptive events or disasters
        - Requires detailed planning and forethought
    - Key Terms
        - *Business Continuity Planning (BC Plan)*
            - Plans and processes for responding to disruptive events
            - Addresses a wide range of threats and disruptive incidents
            - Involves preventative actions and recovery steps
            - Can cover both technical and non-technical disruptions
        - *Disaster Recovery Plan (DRP)*
            - Focuses on plans and processes for disaster response
            - Subset of the BC Plan
            - Focuses on faster recovery after disasters
            - Addresses specific events like hurricanes, fires, or floods
    - Strategies for Business Continuity
        - Consider alternative locations for critical infrastructure
        - Distribute staff across multiple geographic regions
        - Use cloud services to maintain operations during disasters
    - The Role of Senior Management
        - Senior managers are responsible for developing the BC Plan
        - Goals for BC and DR efforts should be set by senior management

        - Appoint a Business Continuity Coordinator to lead the Business Continuity Committee
    - Business Continuity Committee
        - Comprises representatives from various departments (IT, Legal, Security, Communications, etc.)
        - Determines recovery priorities for different events
        - Identifies and prioritizes systems critical for business continuity
    - Defining Scope
        - Senior management decides the plan's scope based on risk appetite and tolerance
        - Can be broken down by business function or geographical area
        - All components must be coherent and compatible for crisis situations

- **Redundant Site Considerations**
    - *Redundant Site*
        - Backup location or facility that can take over essential functions and operations in case the primary site experiences a failure or disruption
    - Types of Continuity Locations
        - *Hot Sites*
            - Up and running continuously, enabling a quick switchover
            - Requires duplicating all infrastructure and data
            - Expensive, but provides instant availability
        - *Warm Sites*
            - Not fully equipped, but fundamentals in place
            - Can be up and running within a few days
            - Cheaper than hot sites but with a slight delay

- *Cold Sites*
  - Fewer facilities than warm sites
  - May be just an empty building, ready in 1-2 months
  - Cost-effective but adds more recovery time
- *Mobile Sites*
  - Can be hot, warm, or cold
  - Utilizes portable units like trailers or tents
  - Offers flexibility and quick deployment (e.g., military DJC2)

- Platform Diversity
  - Critical for effective virtual redundant sites
  - Diversify operating systems, network equipment, and cloud platforms
  - Reduces the risk of a single point of failure
  - Ensures resilience and adaptability in case of disruptions
- Virtual Sites
  - Leveraging cloud-based environments for redundancy
  - *Virtual Hot Site*
    - Fully replicated and instantly accessible in the cloud
  - *Virtual Warm Site*
    - Involves scaling up resources when needed
  - *Virtual Cold Site*
    - Minimizes ongoing costs by activating resources only during disasters
  - Offers scalability, cost-effectiveness, and easy maintenance
- Geographic Dispersion
  - Spreading resources across different locations for higher redundancy
  - Mitigates the risk of localized outages
  - Enhances disaster recovery capabilities

- Considerations for Redundant Site Selection
  - Think about technology stack, people's workspace, and long-term support
  - Determine which type of redundant site suits your organization's needs
  - Ensure continuity of essential functions and services in the event of disruptions

- **Resilience and Recovery Testing**
  - *Resilience Testing*
    - Assess system's ability to withstand and adapt to disruptive events
    - Ensures the system can recover from unforeseen incidents
    - Conducted through tabletop exercises, failover tests, simulations, and parallel processing
    - Helps prepare for events like power loss, natural disasters, ransomware attacks, and data breaches
  - *Recovery Testing*
    - Evaluates the system's capacity to restore normal operation after a disruptive event
    - Involves executing planned recovery actions
    - Performed through failover tests, simulations, and parallel processing
    - Ensures that planned recovery procedures work effectively in a real-world scenario
  - *Tabletop Exercises*
    - Scenario-based discussion among key stakeholders
    - Assess and improve an organization's preparedness and response
    - No deployment of actual resources
    - Identifies gaps and seams in response plans
    - Promotes team-building among stakeholders

- Low-cost and engaging for participants

- *Failover Tests*
  - Controlled experiment for transitioning from primary to backup components
  - Ensures uninterrupted functionality during disasters
  - Requires more resources and time
  - Validates the effectiveness of disaster recovery plans
  - Can identify and rectify issues in the failover process
- *Simulations*
  - Computer-generated representation of a real-world scenario
  - Allows for hands-on response actions in a virtual environment
  - Assesses incident responders and system administrators in real-time
  - Helps evaluate reactions and staff performance
  - Provides feedback for learning and improvement
- *Parallel Processing*
  - Replicates data and system processes onto a secondary system
  - Runs primary and secondary systems concurrently
  - Tests reliability and stability of the secondary setup
  - Ensures no disruption to day-to-day operations
  - Assesses the system's ability to handle multiple failure scenarios simultaneously
  - Uses of Parallel Processing
    - *Resilience Testing*
      - Tests the ability of the system to handle multiple failure scenarios
    - *Recovery Testing*
      - Tests the efficiency of the system to recover from multiple points of failure