



Security+

Domain 3: Security Architecture

Brian Olliff

Defensive Engineering Instructor

Topics

IT Architectures

- **Network**
- **Cloud**
- **VM & Embedded**

Network Security

Secure Communication

Data Protection

Resilient Systems

Learning Objectives

- Understand system architecture concepts
 - + Cloud deployment & service models
 - + Virtualization technologies
 - + Embedded systems (IoT/ICS)
- Explain considerations for architecture options
- Be able to determine secure options for network infrastructure
- Understand different data types & classifications, and how to secure
- Explain infrastructure and system resiliency options
 - + High availability
 - + Planning
 - + Backups

Network Infrastructure



Infrastructure

- Network consists of nodes and links
- Links
 - Physical layer of OSI model (layer 1)
 - Twisted pair, fiber optic, wireless, etc
- Nodes
 - Hosts - normally servers or clients
 - Intermediaries - “typical” network devices
 - Responsible for forwarding traffic on network
 - Switches and routers
- On-premise network/system
 - Installed at a single site/location
 - Operated by a single organization

Infrastructure

- Switches - layer 2
 - Forward frames
 - Most (non-wireless) devices connect via cable to switch
 - All devices have hardware address - MAC address
 - 00-1A-3B-4F-DD-4C
 - Local network segment only - broadcast domain
- Wireless access point - layer 2
- Routers - layer 3
 - Forward traffic between network segments based on IP address
 - Each network segment (normally) has a router - default gateway
- Layer 4 - transport protocols - TCP/UDP
- Layer 7 - application protocols

Segmentation

- Restrict communication between hosts on different network segments
- Physical segmentation
 - Unique network equipment for various subnets/broadcast domains
 - No physical connections between subnets
 - Air-gapped
 - Single or multiple devices with no connection to other network
- Logical segmentation
 - Physically connected to various networks, controls restrict communication
 - VLANs - Virtual LAN
 - Layer 2 segmentation
 - Switch ports can be assigned to VLAN to allow communication

Software-Defined Networking

- Helps to facilitate IaC (Infrastructure as Code)
- Physical and virtual network devices
 - Configured by scripting and APIs
- Network function planes
 - Control plane
 - Decisions about traffic prioritization, security, and switching
 - Data plane
 - Performs switching and routing activities, imposes security controls
 - Management plans
 - Monitors traffic and network status
- SDN used to define policies for network
 - Defined on control plane, implemented on data plane

Cloud Infrastructure



Cloud Deployment Models

- Describes how service is owned and used
- Public
 - Services offered by cloud service providers
 - Subscription or pay-as-you-go
- Private
 - Infrastructure completely private and owned by organization
 - On-premise infrastructure, hosted datacenter services (off-site)
- Hybrid
 - Making use of both on-premise and cloud systems
 - Usually tight integration between systems, especially authentication
 - Additional management and security responsibilities

Deployment Security Considerations

- Multi-tenant
 - Multiple customers share same infrastructure, logical security segmentation
 - Cost-effective, but can increase risk
- Single-tenant
 - Dedicated infrastructure for single customer
 - Highest level of security and control, but more expensive
 - Customer responsible for managing and securing infrastructure
- Hybrid
 - Good combination of security and flexibility
 - Requires careful management for proper integration and security
- Serverless
 - Cloud provider manages infrastructure and scaling
 - Can be more secure, but still requires careful planning

Cloud Service Models

- Infrastructure as a Service (IaaS)
 - Provides virtual (or dedicated) IT resources
 - Servers, switches, load balancers, etc
 - Provides most control and customization
 - AWS EC2, Azure VMs, etc
- Platform as a Service (PaaS)
 - Provides server/storage resources (virtual or dedicated)
 - Access to hosted platform for specific uses
 - Azure SQL DB
- Software as a Service (SaaS)
 - Only provides access to specific software (no servers, IT resources)
 - Microsoft/Office 365, Google Apps, etc

Responsibilities

- Security risks are shared when using cloud services (provider/customer)
 - Cloud provider - hardware/network infrastructure
 - Customer - applications and data
- Responsibilities will vary depending on service model
- Cloud provider
 - Physical and device security
 - Foundational network security (DDos protection, etc)
 - Infrastructure backup and recovery
 - Infrastructure security monitoring and incident response
- Customer
 - User identity management and access control
 - Org-owned data and application security

Responsibility Matrix

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	●	●	●	●	●
Client and end-point protection	●	●	●	●/●	●/●
Identity and access management	●	●	●/●	●/●	●/●
Application-level controls	●	●	●/●	●/●	●/●
Network controls	●	●/●	●	●	●
Host infrastructure	●	●/●	●	●	●
Physical security	●	●	●	●	●

● Cloud Customer ● Cloud Provider

Source: <https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know>



Cloud Service Providers

- CSPs are third-party vendors
 - External entities that provide services, solutions, goods, etc
- Should receive same security considerations other third-party vendors
 - Contract negotiations
 - Service options and performance history
 - Communication practices
 - Security control options (encryption, IR procedures, regulatory compliance)
- Service level agreements (SLAs)
 - Contractual agreement that outlines expected level of service
 - Updates, performance, support response, etc
 - Will also include remedies if service levels are not met
- Switching CSP can be very difficult (sometimes cost-prohibitive)
 - Portability must be evaluated prior to selection

Cloud Architecture



Serverless Computing

- Model where provider manages infrastructure
 - Automatically allocates resources as needed
 - Handle redundancy, load balancing, and provisioning/deprovisioning
- Only charge for resources that are actually used
- Eliminates (reduces) need for managing servers/infrastructure
- All architecture cloud-hosted
 - Services (authentication, web apps, etc) run as functions or microservices
- Uses automation and event-driven orchestration
 - Multiple functions/microservices automatically triggered

Microservices

- Application development through smaller independent services
- Designed to be modular, with single purposes
- Provides ability break down complex programs
- Often uses Infrastructure as Code (IaC)
 - Processes to manage infrastructure using machine-readable configuration
 - Files use formatted code to manage and provision
 - YAML, JSON, etc
 - Information about desired state of infrastructure
 - Config settings, network options, security settings, etc

Centralized vs Decentralized Computing

- Centralized
 - Data processing and storage occur in single location
 - Users and systems rely on central server/system
 - Common to see in enterprise networks
 - Identity management (AD)
 - File, application servers
- Decentralized
 - Processing and storage distributed across multiple systems/locations
 - No single point of failure or source of responsibility
 - Blockchain
 - CDNs

Virtualization



Virtualization

- Multiple systems running simultaneously on a single host computer
- Hypervisor
 - Software that manages and runs virtual machines/systems
 - Type I - installed directly onto hardware as an OS (VMware ESXi)
 - Also known as bare metal
 - Type II - installed on top of already existing OS (VMware Workstation)
- VDI - Virtual desktop infrastructure
 - Uses virtualization to deploy workstations
 - Runs on thin client machines - low powered, low spec workstations
 - Boot with minimal OS and automatically load VM

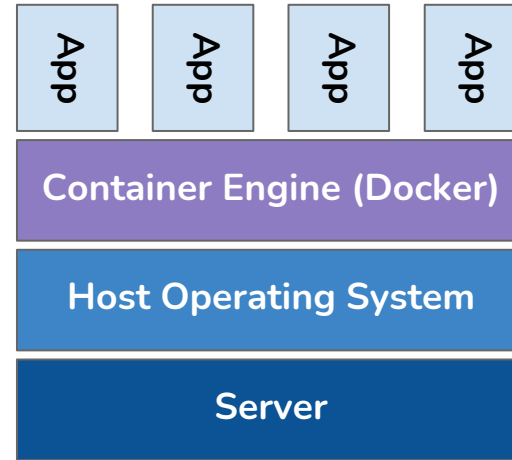
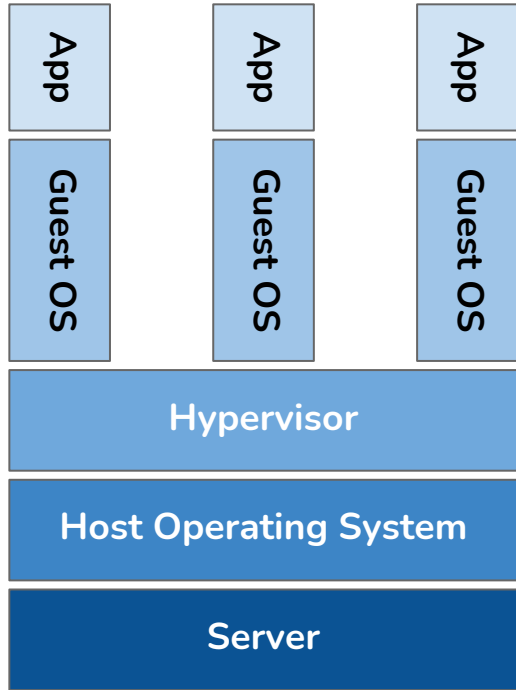
Application Virtualization

- Type of VDI - more limited
- Does not run entire desktop virtualized, but individual applications
- Applications hosted on server
 - Individual virtual instances “streamed” to clients
 - May also be accessed directly on server (still virtualized)
- Most used with HTML5 interfaces (clientless)
 - Can be accessed with standard web browsers
- Citrix XenApp, Microsoft App-V

Containerization

- Form of application-level virtualization
 - Without using standard hypervisor
- Each instance is assigned an isolated “cell” or container
 - Allocated system resources
 - All process run through native OS kernel
 - Can run different versions of software, libraries, etc
- Allow for running various application versions in isolated environments
 - Not full operating systems as containers
- One of most popular - Docker
- Many popular cloud services use containerization

Virtual Machines vs Containers



Virtualization Risks

- VM escape
 - Malware running on guest OS pivoting to another guest or host OS
 - Requires first identifying the system is virtualized
 - Timing attack or system signatures
 - Can result in rapid malware spread
 - Especially in event of hypervisor compromise
- Virtual host/guest management
 - Proper segregation and isolation of guests as needed
 - Critical systems on dedicated, segregated hosts
 - Proper lifecycle and patch management
 - Hosts and guests

IoT & ICS



Embedded Systems

- Computer systems designed to perform specific, dedicated functions
 - Not designed to have software installed/removed
 - Static environment (PC considered dynamic environment)
- IoT - Internet of Things
- ICS - Industrial control systems
- SCADA - Supervisory control and data acquisition
- RTOS - Real-time operating system
- OT - Operational technology
 - Specific network for (normally) industrial applications
 - Normally control physical machinery/devices

Industrial Control Systems

- Designed to control hardware
 - Provide processes for workflow and automation
 - Operate valves/circuits, run motors and other machinery
- Used in critical infrastructure settings
 - Electricity generation, water treatment and pumping
 - Healthcare, telecommunication
 - National security applications
- Work with PLCs (programmable logic controllers)
- Should always be on isolated network
 - Not connected to any other systems unless necessary

SCADA

- Supervisory control and data acquisition
- Systems that run as servers with ICS
- Typically run on standard computers/servers
- Gather data from devices and equipment running PLCs
 - Provide control instructions
- Used in multiple industries
 - Critical utilities
 - Industrial plants (mining, refining, hazardous materials, etc)
 - Fabrication and manufacturing
 - Building systems (HVAC, lighting, dedicated security systems)
- Stuxnet
 - Worm that was designed to attack SCADA software on Windows PCs

IoT

- Appliances/devices with many uses
 - Thermostats, media players, speakers, lightbulbs, watches, smoke detectors
 - Typically with some sort of sensors
- Network connectivity for functionality, management, etc.
 - Usually connected to cloud-based systems
- Security controls difficult to implement on device
 - Lower processing power
 - Designed to focus on functionality instead of security
- Best form of defense is isolation
 - Segmented or dedicated networks (wired or wireless)
- Often attacked and used in botnets for DDoS attacks
 - Mirai botnet

RTOS

- Dedicated OS engineered for specific purpose
 - Flow valves
 - Infusion pumps
- Require high stability levels
 - Predictable response times
 - Stable, high processing speeds
- Low tolerance for crashes or reboots (unscheduled)
- Designed to have small attack surface
 - Still can have vulnerabilities
- Aircraft control, missile guidance, robotics
- Vehicle transmission, safety systems

Security Risks

- ICS/SCADA often manage/control critical systems
 - Failure of connected devices can be devastating
- Frequently use legacy operating systems (Windows XP)
 - May not receive security updates, vendor patches, etc
- Network segmentation is best defense
 - No connectivity to other systems unless required for functionality
 - Management often local on network
 - Secure, hardened workstations

Architecture Considerations



Sizing and Cost

- Cost
 - Purchase, licensing, maintenance, support
 - Value also calculated from incident loss reduction
- Processing power and responsiveness
 - CPU, memory, storage, bandwidth, etc
 - Properly sized and scaled for needed workload
- Power requirements
 - Can existing power infrastructure support additional devices?
 - If not, can infrastructure be expanded?
 - More power usage = increased costs

Performance and Reliability

- Availability
 - Maximize uptime
 - Minimize downtime to scheduled activities (as much as possible)
- Scalability
 - How easy is it to add/remove resources depending on workload?
 - Purchased equipment more difficult to recover cost than cloud-based
 - Difficulty in deploying systems/devices as needed
- Resilience
 - How quickly & effectively a device/system recovers from failure
 - How much manual effort is required to recover
 - Automatic recovery > manual recovery steps

Security & Risk

- Patch availability
 - Vulnerabilities and bugs are corrected in timely manner
 - How are patches delivered?
 - If using third-party for management, no direct control
- Risk transference
 - Contracting third-party to manage infrastructure
 - Frequently implemented with cloud services
 - SLA defined with metrics and penalties

Infrastructure Considerations



Device Placement

- Defense in depth
- Network perimeters
 - Public -> enterprise or between internal segments
 - Firewalls, routers, IPS, etc
- Inside networks
 - Traffic monitoring
 - Detection of malicious activity that evaded perimeter controls
- Endpoints
 - EDR, DLP, HIPS, etc
- Combination of preventive, detective, corrective controls throughout

Security Zones

- Area of network containing hosts with similar security requirements
- Definition requires inventory and risk analysis
- Network segments based on function and access control requirements
 - Data, endpoints segmented based on type of data
 - Public facing servers isolated, no sensitive data stored
- Eliminates “flat network”
 - All devices on internal network are implicitly trusted with same security
- Zones should have known entry/exit points
 - Specific router/interface
- All policies based on least-privilege

Attack Surface

- Any point where an attacker can attempt to exploit a vulnerability
- Varies depending on attacker type (external vs internal)
- Evaluation depends on scope
 - Network - devices, software, management protocols, etc
 - Layer 1/2 - physical ports, broadcast domain (subnet)
 - Layer 3 - IP addresses and routing
 - Layer 4/7 - port and application protections
 - Application - open ports, vulnerabilities, required permissions, etc
 - People - training, level of investment
- Entire infrastructure is attack surface

Failure Mode Options

- What happens when device or system fails?
 - Logs full, hardware fault, software crash, power issue, etc
 - Mostly focused on security devices
- Fail open
 - Operation continues as if device were not present
 - Used when continued functionality is more critical than security
 - Prioritizes availability over confidentiality and integrity
- Fail closed
 - When failure condition present, device locks down
 - Used when security is more critical than functionality
 - Prioritizes confidentiality and integrity over availability
- Choice depends on organization's risk appetite

Device Types

- Active security control
 - Often uses agent installed on endpoint for scanning/filtering
 - Requires credentials/access permissions for client-host data exchange
- Passive security control
 - Does not require any agent or client-host data transfer
 - Collection of network traffic from switch
- Inline
 - Device inserted into communication path
 - Does not require changes to network topology
 - TAP - copies signal from cable to monitor device
- Monitor
 - SPAN/mirror - specific monitor port configured to copy traffic to sensor
 - Less reliable than inline, traffic may be dropped during heavy load

Network Security



Intrusion Detection & Prevention

- Network sensors used to capture traffic
 - SPAN/mirror port or inline TAP
 - Normally placed “nearby” device of interest (firewall, server, switch, etc)
- Intrusion Detection System (IDS)
 - Software/appliance that performs real-time analysis of network traffic
 - Host-based (HIDS) or network-based (NIDS)
 - Passive detection only - does not take any action on traffic
 - Alerts and notifies
- Intrusion Prevention Systems (IPS)
 - Similar to IDS, but with additional capabilities
 - Provides active response in addition to alerting and notification
 - Block traffic - permanent or temporary
 - Reset connection, but not block
 - Redirect to honeypot/net for further logging & analysis

Firewalls

- Stateless vs stateful inspection
- Web application firewall (WAF)
 - Designed specifically to protect web servers (and backend components)
 - Code injection, DoS attacks, etc.
 - Application-aware filtering
 - Can use signature-based or pattern-based detection
- Layer 4/Layer 7
 - Transport and Application layers (OSI model)
 - Layer 4 checks for proper 3-way handshake
 - Layer 7 check various application protocols (headers, code, etc)
 - Unencrypted only (unless paired with SSL/TLS inspector)

Firewalls

- Next-generation firewall (NGFW)
 - Upgrade from early packet-filtering firewalls
 - Introduced additional features
 - Connection-aware and user-based filtering
 - Integrate with user directories
 - IPS functionality
- Unified threat management (UTM)
 - Single product that contains multiple controls - expansion of NGFW
 - Firewall, anti-malware, IPS, spam filtering, VPN, etc)
 - Single management point for multiple controls
 - Must be properly sized/configured to avoid latency
 - Also potential single point of failure

Network Appliances

- Jump server (box)
 - Dedicated administrative workstation
 - Locked down/hardened to only allow specific traffic and uses
 - Usually only allows traffic on dedicated management ports (SSH, RDP, etc)
 - Servers restricted to only allow admin connections from jump boxes
 - Frequently used to manage secure zones
- Load balancer
 - Appliance that distributes traffic across multiple destinations
 - Layer 4 & layer 7
 - Used for fault tolerance and redundancy to ensure availability
 - Also can be used for DDoS mitigation
 - Round robin, fewest connections, fastest response

Proxy Servers

- Work on store-and-forward model
 - Ingests packets, deconstructs for analysis, rebuilds and forwards
 - Forwards only if no rules that would otherwise drop/block
- Forward proxy
 - Typically used with web traffic - analyzes, filters, modifies traffic
 - Other protocols used also
 - Outbound traffic from client
 - Transparent - router configuration or inline appliance
 - Non-transparent - client configuration to send traffic through proxy
- Reverse proxy
 - Inbound traffic, typically in front of public servers (web, email, etc)
 - Filtering rules to analyze, modify/block inbound traffic

Port Security

- Switch ports and physical devices always physically secured
- Most basic method - disable unused ports
 - High level of management overhead, easily for attackers to get around
- MAC filtering
 - Allow list of specific MAC addresses permitted to connect
 - Only permit specific number of MAC addresses per port
 - Management overhead and easy to spoof known MAC to evade restriction
- Authentication models to allow connection
 - 802.1X
 - EAP
 - RADIUS

802.1X Authentication

- IEEE 802.1X Port-based Network Access Control (PNAC)
- Uses AAA architecture (authentication, authorization, accounting)
 - Supplicant - device attempting to connect
 - Authenticator - device attempting to connect to (switch, etc)
 - Authentication server
- Two protocols used for authentication
 - Extensible Authentication Protocol (EAP)
 - Frequently used with digital certificates to establish trust
 - Can use multiple types of authentication
 - Remote Authentication Dial-in User Service (RADIUS)
- When connecting, switch allows only EAP protocol traffic
 - Receives supplicant credentials via EAP (encrypted)
 - Uses RADIUS to send to authentication server

Secure Communications



Remote Access

- Connecting to a network through an intermediate network
- One of original ways - dial-up modem using telephone lines
- Current methods
 - VPN technologies
 - TLS/IPSec
 - Remote desktop
 - Secure shell (SSH)
- Security recommendations
 - Secure, encrypted connection
 - Limited availability (least privilege)
 - Multi-factor authentication

Remote Desktop

- Uses graphical tools to connect to individual (or virtual) desktop
- Microsoft Remote Desktop Protocol (RDP)
 - Commonly used for single desktop connections inside network
 - If used remotely, **NEVER** open RDP ports to internet (3389)
- Remote desktop gateway
 - Provides access to virtual desktops through secure interface
 - HTML5 supports remote desktops in browser
- Various third-party applications exist
 - TeamViewer, VNC, etc

VPN

- Virtual Private Network
- Client-to-site VPN
 - Software installed on client computer connects to VPN gateway
 - Remote worker model
- Site-to-site VPN
 - Two VPN gateways establish trust and secure connection
 - Requires no endpoint/client configuration
- Establish secure “tunnel” to keep communication private
 - Point-to-Point Tunneling Protocol (PPTP) - deprecated, insecure
 - Transport Layer Security (TLS)
 - Internet Protocol Security (IPSec)

TLS Tunneling

- Client connects to remote access server
- Uses digital certificates
 - Server certificate identifies VPN gateway
 - Client certificate authenticates endpoint (not required)
 - If both used - mutual authentication
- Encrypted tunnel to then submit authentication credentials
- Verify version of TLS in use
 - Older versions not as secure as newer versions
 - TLS 1.3 newest, 1.2 still supported (currently)

IPSec

- Two core protocols
 - Authentication Header (AH)
 - Performs hash on entire packet, with pre-shared key, & adds to header
 - Integrity Check Value (ICV)
 - Not encrypted - no confidentiality provided
 - Encapsulating Security Payload (ESP)
 - Encrypts packet
 - Attaches 3 fields to packet - header, trailer, ICV
- Two modes
 - Transport mode
 - Secure communication between hosts on private network
 - Tunnel mode
 - Communications across unsecure network (VPN)

Other Secure Access

- Software-defined Wide Area Network (SD-WAN)
 - Routing and tunnels managed by software
 - Can connect offices, data centers, cloud infrastructure, etc over WAN
 - Encrypted tunnels for secure communication
- Secure Access Service Edge (SASE)
 - Combines WAN and cloud security
 - Provides secure access to cloud applications/services
 - Useful for securely accessing cloud services regardless of location
 - Uses zero trust model for security
 - All users/devices untrusted until proven otherwise

Data Types



Regulated Data

- Data subject to legal/regulatory requirements
 - Handling, storage, protection, etc
- PII
 - Personally identifiable information
 - SSN, DL, name/address/DoB, CC#s (PCI-DSS)
- PHI
 - Protected health information
 - US - HIPAA (Health Insurance Portability and Accountability Act)
- Regulations and requirements vary by location

Intellectual Property

- Often abbreviated as IP
 - Referred to as proprietary information as well
- Data/information created by the organization
 - Normally relates to products or services
- Frequently targeted by competitors and/or nation-state actors
 - Government IP targeted by foreign governments
- Copyrights and trademarks
 - IP is often copied or duplicated for counterfeit purposes
- Trade secrets
 - Specific type of IP - recipes, formulas, etc
 - Commercial value
 - May require NDAs to access (non-disclosure agreement)

Financial Information

- Customer/client information
 - Bank/investment account information
 - Account & routing numbers
 - Credit card information
 - Including expiration dates and CVV numbers
- Organization financial data
 - Performance, activities, statements, reports, tax records, etc
- Legal data
 - Contracts, documents, litigation info - any legal documents
 - Governance/compliance, legal obligation information, etc

Data Readability

- Human-readable data
 - Information that can easily be read by people
 - Text, images, videos, etc
- Non-human-readable
 - Information that is not easily understood by people
 - Machine-readable data
 - Binary code, machine code, encrypted data, etc
 - Requires some sort of processing to convert to human-readable
- Each requires different forms of security controls
 - Human-readable - web filtering, DLP, user training
 - Non-human readable - access controls, encryption, IPS, etc

Data Classification



Classification

- Different types of data need different levels of protection
 - Primarily based on degree of confidentiality required
 - Can be expensive to equally protect all data at highest level
 - More protection may also increase complexity in accessing
- Usually performed using classification labels
- Manual classification
 - Users apply labels as data is created/accessed
- Automatic classification
 - Systems apply labels based on contents/location/metadata
 - Users may have option to modify (or request modification)

Classification Based on Confidentiality

- Public (unclassified)
 - No restrictions on viewing data
 - Would pose no risk to the organization if released
 - Potential risk if modified without authorization, or not available
- Confidential (secret)
 - Sensitive data, only viewable by approved individuals in organization
 - Can also be permitted for third-parties under specific agreements (NDA)
- Critical (top secret)
 - Extremely sensitive, cannot be disclosed under any circumstances
 - Significant restrictions on access
 - Very high risk to organization if disclosed

Classification Based on Information Type

- Proprietary (intellectual property)
 - Information created, owned by company
- Private data
 - May also be labeled as “personal data”
 - Usually relates to individuals
 - Financial information, SSN, health info, etc
 - PII, PHI (these may fall under other labels as well)
- Sensitive
 - Usually used in context of personal data (but not always)
 - Information that could harm individual if disclosed
 - GDPR has specific definition
- Restricted
 - Confidential data with limited access/strict access controls

Securing Data



Data Considerations

- Data sovereignty
 - Jurisdiction may prevent or restrict data processing and storage
 - May require that data physically reside within jurisdiction (country)
 - GDPR - any EU citizen's data, regardless of org location collecting/processing data
- Geolocation
 - Storage locations for data may be subject to specific regulations/laws
 - Possible restrictions on storage, replication, backup locations
 - May impact incident response activities depending on regulations
 - Cloud providers often allow choice of where to store data
 - Employees may need access from multiple locations
 - Access from specific locations may require additional verification

Data States

- Data at rest - data stored on persistent storage
 - Files stored on server
 - Data stored within database tables
 - Backups or archives
- Data in transit (in motion) - in process of being transferred over network
 - Website traffic
 - VPN/RDP traffic
- Data in use - data present in volatile memory (RAM, CPU, etc)
 - Open documents, database being modified
 - Normally encrypted data, decrypted for use
 - Event logs being generated

Securing Data

- Encryption
 - Encrypted data cannot be read without decrypting
 - Protects from unauthorized access and modification (confidentiality)
- Hashing
 - One way mathematical function to verify data integrity
- Masking
 - Redacting all or some of information
 - Ex: replacing digits in phone number with X
- Tokenization
 - Replacing portions of data with randomly generated tokens
 - Token stored with original value on separate server
 - Not same location as normal file storage
 - Authorized apps/processes can retrieve original value

Securing Data

- Permission restriction
 - Access controls to restrict access to files/data
 - ACLs (access control lists) in OS (Windows)
 - RBAC (role based access control)
- Segmentation
 - Network & system segmentation
 - Splitting larger networks into smaller, isolated ones
 - Helps limit impacts of breach/intrusion
- Obfuscation
 - Altering data to make it more difficult to interpret
 - Hashing, data masking, etc
- Geographic restrictions
 - Limiting access to data based on physical location

Resilient Architecture



High Availability

- Resilient systems require minimal downtime (highly available)
- Accomplished through redundant infrastructure
- Measured by percentage of time systems are available
 - “5 9s uptime” - available 99.999% of the time (avg downtime ~5 min/year)
- Load balancing
 - Spreading workload between multiple resources
 - Can provide failover functionality
 - Network, server, application, etc
- Clustering
 - Multiple servers sharing the same data & session info
 - Allows seamless failover
 - DB server, email servers, etc

Clustering

- Virtual IP
 - “Shared address” or “floating address”
 - Single IP that is shared among cluster members
 - Each device still has its own IP - “real” IP
- Active/Passive
 - One node in cluster active processing, other is “standby”
 - No performance effects during failover - unused resources
- Active/Active
 - Both nodes process at the same time
 - Maximum processing capacity during normal operations
 - Performance degraded during failover
- Clustering can apply to applications as well as devices/servers

Site Resiliency

- Resiliency & high availability can be accomplished using multiple sites
 - Distributing workloads among multiple sites
 - Using multiple sites for failover and DR
- Geographic location of sites is important
 - Sites located nearby
 - Useful for equipment failures, data loss, localized disasters
 - fire, small area power outages, localized weather events, etc
 - Sites located large distances from each other
 - More useful for severe issues
 - Large-scale natural disasters (earthquakes, hurricanes)
 - Widespread power outages

Site Classifications

- Hot site
 - Near instant failover
 - Systems online with current data and readily available
 - High cost, minimal downtime
- Warm site
 - Systems online (or ready to bring online), may need data to be updated
 - Lower cost, possibly longer downtime
- Cold site
 - Systems may not be present, only location available
 - Lowest cost, longest downtime

Diversity

- Defense in depth
 - No single control can protect 100%
 - Multiple layers of security using various products
- Platform and vendor diversity
 - “Don’t put all your eggs in one basket” - risk reduction
 - Multiple vendors, applications for various purposes
 - Ex: Cisco for network, Palo Alto for firewall, Sophos for EDR
 - Different systems will have various vulnerabilities, level of difficult to exploit
 - Vendors have different levels of security, innovation, features, customization
- Cloud diversity
 - Compromise/outage at one vendor will not affect the other
 - Each may have unique security controls, costs, uptime, features, etc

Power

- Multiple methods to implement redundant power
 - Depends on needs, budget
- Dual power supplies
 - Most enterprise equipment includes 2 power supplies
 - Protects against single point of failure
 - Connect to different circuits
- Uninterruptible power supply (UPS)
 - Battery backup that equipment connects to (or integrated within)
 - Provides temporary power in event of outage
- Generators
 - Various types of fuel (diesel, gasoline, propane, natural gas)
 - Can often supply electricity for multiple days
 - Depending on size, fuel capacity/availability, etc

Business Continuity



Continuity of Operations

- Ensuring org can maintain/quickly resume operations after disruption
 - Minimize downtime, maintain resilience
- Focuses on critical functions during emergency
- Business continuity
 - Resilience and recovery of entire organization - broader overview
 - Risk assessments, mitigations, plan/documentation to recover
 - Supply chain management, employee communication, legal, etc
- BCP (Business continuity plan)
 - Documentation that defines how organization should deal with disruption
 - Minor disruptions or major outages/disasters
 - Addresses required resources (hardware, personnel, location, etc)
 - Timelines on restoration

Capacity Planning

- Process to determine required resources to meet objectives
 - Current and future
 - Forecasting to anticipate future growth & changes
- People
 - Number of employees, skill sets, training
 - Eval productivity, staffing levels, skill gaps
- Technology
 - Hardware, software, network resources for business operations
 - Supporting required performance, reliability, and potential scalability
- Infrastructure
 - Physical facility requirements
 - Power, cooling, connectivity
 - Possibility for expansion or relocation of systems/people

Addressing Planning Risks

- Cross-train employees in other job roles
- Ensure adequate planning for remote work when needed
- Establish alternate reporting structures
- Effective communication plans, channels, & methods
 - Communication during outages/disasters among incident responders
 - Plans for effective communication for rest of organization
- Risks from workforce reduction
 - Insider threats & concerns from former employees
 - Lack of expertise and knowledge
- Proper infrastructure planning to ensure operations
 - Server/network capacity
 - Security controls to protect environment
- Caution against overestimating needs

Resiliency Testing

- Tabletop exercises
 - Simulated incident (ransomware, physical disaster, etc)
 - Personnel use documented procedures to “respond” to incident
 - Depending on incident, personnel from across organization
 - Provide practical testing of policies and procedures for DR/BC
- Failover tests
 - Intentionally causing primary systems to fail (non-destructively)
 - Evaluate automatic transfer to secondary systems
 - Transfer time - minimal downtime & data loss

Resiliency Testing

- Simulations
 - Similar to tabletop exercises, but replicate scenarios
 - Designed to test IR processes and plans
 - Potentially identify flaws in plans/documentation
 - May not be identified in tabletop
- Parallel processing
 - Run primary and secondary/backup systems simultaneously
 - Test backup systems, without taking primary down
 - Evaluate functionality and performance without disruption
 - Data processing, network operations

Backups



Backups

- Data is important to any organization
 - Data will inevitably be corrupted or lost
- Policies and procedures are required
 - What data is backed up
 - How often backups occur and are tested
 - How that data is restored when needed
- System tiering is often used
 - Most critical systems have priority, may be backed up more often
- Backup considerations
 - Type of backup
 - Destination
 - Frequency
 - Retention

Frequency of Backups

- “Typical” backup frequencies
 - Annual, monthly, weekly, daily
- Frequency determined by various needs
 - Data volatility
 - Regulatory requirements
 - Operational needs
 - Infrastructure capabilities
- Stable data usage, less regulatory requirements
 - May need less frequent backups
- Dynamic data usage, stricter regulations
 - More frequent backups needed

Backup Storage

- Onsite
 - Backups stored locally (same location as production systems)
 - Hard drives, tape backups, etc
 - Useful when rapid recovery is important
- Offsite
 - Backup data transferred to remote location
 - Provides protection against physical risks
 - Natural disasters, theft, power outages, etc
 - Longer recovery times
- Replication to other storage or another site/location
 - Provides redundancy for backups (backup of backup)

Advanced Backup Strategies

- Snapshots
 - Captures state of system/data at a specific time
 - VM, filesystem, SAN, etc
- Replication
 - Exact copies of data on different systems/different locations
 - SAN, VM, database, etc
 - Can provide granular, rapid recovery
- Journaling
 - Records changes to data in a separate log - journal
 - Track changes over time & revert if/when needed
 - Provides very granular recovery options
- Encryption
 - Data privacy, security, compliance, etc

Backup Recovery

- Validation and testing
 - Ensure recovery/restore of backups functions properly
 - Verify/validate plans and documentation
- Full recovery test
 - Restore entire system to test environment
 - Verify functionality
- Partial recovery test
 - Restore files/folders/databases
 - Verify integrity of restored items
- Simulate disaster scenarios to gain insight into process
 - Recovery effort and time required
 - Gaps in plans and documentation