CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-8-using_resiliency_and_automation_to_reduce_risk
Title: Using Resiliency and Automation to Reduce Risk
Subtitle: CompTIA Security+ (SY0-501)

3.8 Using Resiliency and Automation to Reduce Risk

- 3.8 Explain how resiliency and automation strategies reduce risk.
  - Automation/scripting
    - Automated courses of action
      - Timely cost-effective
      - Automated actions provide consistency and can reduce the element of human (provided the automation is setup appropriately)
    - Continuous monitoring
    - Configuration validation
  - Templates
    - Reducing time to deployment
    - Configuration baseline
  - Master image
    - Centralized:
      - Patch Management
      - OS Upgrading
      - Configuration Management
      - Consistency
      - Secure State
      - Beneficial in non-persistance
      - Repository of master images to deploy based on employee roles
      - Coupled with policies the company control the environment
  - Non-persistence
    - Snapshots
      - Great for testing environments
    - Revert to known state
      - System Restore
      - System state backups
    - Rollback to known configuration
    - Live boot media
      - Memory resident operating systems
      - No requirement to install to local media
      - Test OS before implementing it
      - Allows a user to work with a computer that is not their own
      - Use the live environment to recovery important data when the host OS fails
  - Elasticity
    - Elasticity allows a company to scale out and/or up when there is an increased demand for resources.
    - Elasticity allows for the rapid deployment and provisioning of vital resources on-demand
    - Elasticity allows for rapid deprovisioning when a resource or group of resources are no longer necessary
    - Allowing for on-demand availability
    - Reducing risk of overprovisioning
    - Reducing the risk of unavailability
  - Scalability
    - Scalability allows an organization to adapt to increase workloads, by adding resources but not necessarily on demand
    - Scalability by itself cannot reduce the risk of overprovisioning when the workload is reduced or the provisioned resources are no longer needed. (Stuck with the cost of a server for example)
    - Scaling out vs. Scaling up
  - Distributive allocation
  - Redundancy
    - Storage Devices
    - Network devices
      - Routers and Routes
      - Switchs
      - NLBs
      - Firewalls
      - Cabling or Connections
      - APs
    - Services
      - Domain Controllers
      - DNS Servers
      - File Servers
      - Cloud providers
      - ISPs
  - Fault tolerance

- High availability
  - How close can a provider get to 100% uptime
  - See diagram
- RAID
  - 0, 1, 5, 10,50
  - See diagram