A Risk Analysis/Assessment For ServiceNow with Risk Mitigation Suggestions and Cost Benefit Analysis

COSC 4364 | Group 1

Jakob Hoisington
Darius Richardson
Ethan Huynh
Kenny Gomez
Sandhya Malla

An Intro to servicenow

- American cloud computing platform
- Provides management solutions and other related products
- Initially worked as a cloud IT management service provider
- Has grown in size and scope to offer generalized business operations management solutions
- Rapid growth has earned ServiceNow a name for themselves

Asset/Infrastructure Identification

ServiceNow has a variety of assets that make up their infrastructure. Some key assets are:

- Website
- Cloud module suites they offer
- In-house databases
- Provided cloud services/platform infrastructure
- Proprietary API for use with ServiceNow
- Physical Assets located on site

Asset Criticality

From most critical to least

- Cloud platforms/infrastructure provided
- Cloud services provided
- Different module suites
- In-house databases
- Proprietary API
- Website

Potential Threats/Risks

- Must be TX-RAMP certified
- Platform upgrades must be monitored
- Backdoor account
- Possibility of bypassing module segregation
- What types of data are hosted presents its own risk

Threat Value Assessment

The Threat Value Assessment is too large to paste into a single slide.

Risk Assessment using RIIOT

Focus on two primary assets:

1. **Desktop Computers:** Used by staff and personnel daily.
2. **Personal Devices:** Laptops, smartphones, tablets, mainly electronic devices used by employees and contractors to access the networks utilized by ServiceNow.

Assumptions:

- Threat actors will possess basic technical knowledge.
- There are basic security measures such as firewalls, antivirus, etc.
- The impact of a breach will be financially high.
- The possibility of threats will be influenced by the specific usage patterns within ServiceNow.
- Policy and procedure documents have been reviewed prior and are used as a supplement during this security risk assessment.

Reviewing Threats

Threats to Desktop Computers:

- Malware Infection
- Unauthorized Access
- Hardware Failures
- Device Theft

Threats to Personal Devices:

- Lost or Stolen
- Malware Infection
- Insufficient Security

Interviewing Key Personnel

Desktop Computers:

- Meet with InfoSec staff
- Meet with general users
- Meet with policy drafters

Personal Devices:

- Meet with general users

Inspecting Device Security for Compliance with Policy

After conducting interviews, it’s important to inspect current device security implementations in order to determine policy compliance

Observe Personnel for Policy Compliance

It’s important to observe personnel behavior to determine current policy comprehension/how well staff is following policy and to determine current user security awareness/mindfulness

Test Security Measures

Testing comes in two matters:

1. Vulnerability identification
2. Penetration testing

These two matters help ensure current safety measures in place are working and are robust

Risk Mitigation Methods

Policy Changes:

- Password Complexity
- Access Control Lists
- Incident Response Protocol

Technical Solutions:

- Workflow Automation
- Role Based Access Control
- Medium-Access-Control Filtering/Monitoring
- Intrusion Detection and Prevention Systems

Physical Solutions:

- Guards/Cameras/Monitoring Stations
- Gates/Fences/Doors with Coded Locks

Organizational Solutions:

- Two Factor Authentication
- Security Training/Awareness

Cost Benefit Analysis

Policy Changes:

- Password Complexity
  Cost: Time and effort to implement stricter policies
  Benefit: Reduced risk of intrusion
- Access Control Lists
  Cost: Time spent reviewing and adjusting ACLs
  Benefits: Improved data security.
- Incident Response Protocol
  Cost: Time, effort, and expertise in forming the IRP
  Benefits: Having an IRP

Physical Solutions:

- Guards/Cameras/Monitoring Stations
  Cost: Hiring personnel, investing in security equipment
  Benefit: Deterrence of physical intrusions
- Gates/Fences/Doors with Coded Locks
  Cost: Installation and maintenance of physical barriers
  Benefits: Physical access control, deterrence of physical intrusions

Technical Solutions:

- Workflow Automation
  Cost: Initial setup and configuration along with potential training for staff
  Benefits: Increased operational efficiency and reduced human error
- Role Based Access Control
  Cost: Defining and assigning roles (effort and time)
  Benefits: Granular access control, reducing risk of intrusion
- Medium-Access-Control Filtering/Monitoring
  Cost: Implementation and maintenance of MAC filtering system, potential hardware investment.
  Benefits: Increased network security.
- Intrusion Detection and Prevention Systems
  Cost: Setup and maintenance alongside potential training
  Benefits: Increased network security

Organizational Solutions:

- Two Factor Authentication
  Cost: Implementation and potential user training
  Benefits: Enhanced authentication security
- Security Training/Awareness
  Cost: Time and effort put into security awareness training and materials development.
  Benefits: Improved employee awareness and behavior towards security

Conclusion