SECURITY AT THE FOREFRONT

OBJECTIVES

- Discuss why security should always be a discussion point
- Understand why how security can make or break a project or system

SECURITY FIRST!

- As system administrators, security needs to remain the top thought
- Everything we install, remove, configure, etc. might make the system insecure
- There is no such thing as a secure computer!
- What is secure at one moment, might not be the next

PRE-SYSTEM DEPLOYMENT ANALYSIS

- Before a system is put into place, security must be thought about
- What will the system do
- Will it be a secure deployment
- Who will manage it
- Is there a plan for disaster recovery
- Is there a support plan

SYSTEM OPERATION ANALYSIS

- Systems constantly need assessment to ensure they are secure
- Are patches applied on time
- Is antivirus running
- Are backup and DR processes monitored and running
- Have we tested a DR plan
- Is there a change process in place

POST SYSTEM ANALYSIS

- Has critical data been migrated to a new host
- Has sensitive data been wiped
- Are we treating the system sustainably so that the parts don't end up in the landfill

CONCLUSION

- Security needs to be integrated into the entire system management process!
- Throughout the next few lessons we will cover these topics in depth

ATTACK SURFACES

OBJECTIVES

- Understand what attack surfaces are
- Discuss how to find them
- Discuss ways to mitigate them

ANATOMY OF SYSTEMS

- Systems generally have:
  - Hardware
  - Operating system
  - Software
  - Users
  - Location
- Each area of a system might be a way for an attacker to get in

ATTACK SURFACES EXPLAINED

- A good analogy is your home. A typical home has:
  - Windows
  - Doors – both inside and outside
  - Vents to the outside
- If someone leaves a door or a window open – what would happen? Someone might break in
- Attack surfaces are ways that an attacker can compromise a system

COMMON AREAS OF INTRUSION

- Insecure passwords
- Management ports left open
- Configuration pages accessible
- Vulnerable services that are accessible
- Users with more access than they should have

3 KINDS OF ATTACK SURFACES

- Network – ports left open to services
- Software – services themselves
- Human – social engineering, configuration errors, questionable and ethical issues

MITIGATING ATTACK SURFACES

- Network based attacks
  - Reducing amount of ports open
  - Segmentation
- Software based attacks
  - Reducing amount of code executing on systems
  - Performing least privilege and/or implementing access control mechanisms
  - Limit the damage
- Human based attacks
  - Least Privilege
  - Constantly evaluate what a user needs access to
  - Separation of duties

CONCLUSION

- Attack surfaces may be numerous
- It's important to list out what attack surfaces you have and how to mitigate each

INTEGRITY

OBJECTIVES

- Explain what integrity is in system management
- Understand why integrity will get you places in your career
- Discuss why a system administrator's integrity can translate to system integrity

WHAT IS INTEGRITY

- I'm not talking about the "I" in CIA triad
- I'm talking about person integrity defined as being an honest person and having moral principles
- My boss, who is the CIO, has said many times, "If you tell the truth, you only have to remember one version of it"

WHY INTEGRITY MATTERS

- Personal integrity within the computer science field can be challenging, both for a system administrator and others who use your systems
- Personal integrity can be compromised if you are not honest
- Computers can always find you out, no matter who you are
- Try to hide something and you will be found out

INTEGRITY IS IMPORTANT

- It is in the code of conduct for ACM and IEEE and many other professional organizations
- **ACM – Code of Conduct 2.6 Honor contracts, agreements, and assigned responsibilities.**
- Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

CONSEQUENCES

- If someone does not posess and practice integrity:
  - Systems may fail
  - Data breaches may occur
  - Careers are destroyed
  - There may be loss of life and property
- Government jobs depend on integrity

ISSA – INFORMATION SYSTEMS SECURITY ASSOCIATION CODE OF ETHICS

- "As an ISSA member, guest and/or applicant for membership, I have in the past and will in the future:
- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of or is detrimental to employers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers."

CONCLUSION

- Ethics and integrity will serve you more than you will ever know
- Even if you are facing your boss and are on the verge of a firing – have integrity
- Own up to your mistakes

POLICIES – PART 1
ORGANIZATIONAL POLICIES

OBJECTIVES

- Understand what organizational policies are
- Discuss how organizational policies can help with security
- Differentiate different types of policies
- Disseminate where you can obtain “fill in the blank” policies

ORGANIZATIONAL POLICIES

- Organizational policies give direction to employees and users about security
- They are rules that are to be followed
- Policies are different than procedures and standards in that procedures are meant to be followed and ignorance of policy can lead, in some cases, to termination
- Policies are stronger than best practices
- Organizational policies are documents that you can go back to and audit to ensure security measures are kept
- They provide the foundation for technical controls

WHAT ALL POLICIES SHOULD CONTAIN

- Effective date
- Approvers
- Responsible party
- Primary Contact
- Related Policies
- Last Revision date

ORGANIZATIONAL POLICIES SHOULD:

- Not contain specific technology or companies
- Not contain how to implement the policy
- Be reviewed periodically – every 3 years or when circumstances change
- Be used for auditing to ensure rules are followed
- Be disseminated to a large group
- Vetted by stakeholders

EXAMPLES OF TYPICAL POLICIES

- Acceptable Use Policy
- Clean Desk Policy
- Data Breach Response Policy
- Email Policy
- Ethics Policy
- Security Policy
- Privacy Policy

EXAMPLES OF SPECIFIC POLICIES

- Remote Access Policy
- Wireless Communication Policy
- Technology Equipment Disposal Policy
- Data Center Security Policy
- Software Installation Policy

AUP – ACCEPTABLE USE POLICY

- Also known as Responsible Computing Policy in some organizations
- Outlines responsibilities of users and employees of an organization
- Topics covered generally include:
  - Acceptable usage of computing resources
  - Prohibited uses of computing resources
  - Privacy
  - Violations

SECURITY POLICY

- Usually a large document
- Defines responsibilities of employees, users and service providers to maintain security of systems
- Defines what information should be protected
- Defines reporting structure if there is a breach or loss
- Can define information classification

CONCLUSION

- Organizations and enterprises need policies to guide and steer what they do
- Public also wants to know what protects privacy
- Policies should be visible to everyone so they can stand up to tests of wills

POLICIES – PART 2 TECHNICAL POLICIES

OBJECTIVES

- Understand the difference between technical policies and organizational policies
- Explain where technical policies might be configured
- Give examples of types of technical policies

TECHNICAL POLICIES

- Policies that actually allow or deny users from doing something
- Policies that configure systems
- Configuration items

TECHNICAL VS. ORGANIZATIONAL POLICIES

- Organizational policies tell us why we do things
- Technical policies enforce them
- Both types of policies go hand in hand
- Example: Password policy
  - Organizational policy may say: Can not use the last 5 passwords due to password reuse concerns
  - Technical policy actually configures this policy in an Active Directory domain

WHERE YOU MIGHT FIND TECHNICAL POLICIES

- Active Directory within a Windows Domain
  - With Group Policies – we can restrict or allow a number of technical policies – 100's in fact
- Software configuration pages
- Hardware configuration pages
  - Firewalls – limiting sensitive content based off certain criteria

CASE STUDY: PCI

- Payment Card Industry Data Security Standards have 12 requirements
- These are a great example of organizational policies mapping to technical policies
- Nearly all 12 requirements address what organizational policies should cover
  - Requirements 1-11 can also be technical policies you may implement

EXAMPLES OF TECHNICAL POLICIES

- Passwords
- Encryption
- Anti-malware
- User accounts
- Backups
- Disaster Recovery controls

CONCLUSION

- Both technical and organizational policies are important
- Technical policies should also be used in case of incidental exposure and intentional activities

SEPARATION OF DUTIES

OBJECTIVES

- Explore case study where separation of duties might be needed
- Understand how auditing is critical to successful implementation and ongoing operating
- Understand how daily operation is performed and different than auditing

CASE STUDY – SENSITIVE DATA

- You are a system administrator that is working on credit card processing systems
- It's your job to maintain the systems along with 2 others on the team
- You notice that ports are turned on to the system one day
- One of your other system admins says they needed to open it for just a few minutes to move some files
- Did something happen?

CASE STUDY – QUESTIONS TO ASK

- Since you know the system, should you investigate or if you think something is not right, report it?
- Should an impartial entity look at the system?
- Do you think that your colleagues will think you are doing your job if you investigate?
- If someone else was in charge of investigating and auditing systems, would you or the other system administrator be worried?

SEPARATION OF DUTIES

- Separation of duties allows 2 parties, groups, teams, or individuals to both maintain systems and audit them
- Each party acts impartially, typically reporting to another division
- These checks and balances ensure both fairness and higher security than just one party doing both jobs
- It helps eliminate conflicts of interest

IMPORTANCE OF AUDITING

- Auditing allows us to ensure systems are run the way that they were intended
- PCI – auditing is commonplace, ensuring systems are maintained per requirements
- HIPAA – auditing ensures least privilege and records are not leaked
- Auditing ensures that integrity is intact

IMPORTANCE OF DAILY OPERATION VS. AUDITING

- While auditing in a sense is ensuring the system is working as intended, in this case, auditing ensures we are above reproach and have non-repudiation
- Auditing ensures someone cannot deny the truth about the status of a system
- System administrators need to perform audits on their system, but who checks if they are telling the truth
- Impartial third parties or different internal departments, such as audit department, perform this task

EXAMPLES OF AUDITS

- Risk assessments
- PCI-DSS audits
- Penetration tests
- HIPAA audits

CONCLUSION

- Separation of duties allows us to have checks and balances
- When planning for systems, ensure critical systems especially financial systems have separation of duties in mind

PLANNING FOR DISASTER

OBJECTIVES

- Understand that disasters can happen anywhere and at any time
- Discuss different disaster plans and where to obtain information
- Understand how a disaster can be planned for

DISASTERS ARE INEVITABLE!

- During the Fukushima nuclear disaster in 2011, not only did the world witness a nuclear disaster, but an IT disaster
- Nuclear disaster really wasn't the main issue, it was flooding
- Hard drive prices skyrocketed because 40% of the world's hard drives were manufactured in Thailand
- How do you plan for something like that!

NATURAL DISASTERS

- Most common natural disasters that affect IT:
- Earthquakes
- Flooding
- Storms – lightning, tornados
- Fires
- Tsunamis

CYBER ATTACKS AND INSECURITY

- Hackers
- Hacktivists
- Accidental exposure
- Misconfigurations
  - Amazon – 15 minute outage estimated to cost $140 million loss

CASE STUDY

- Waldo Canyon fire in Colorado Springs
- We watched from the 3rd floor of the library as the fire crested over the mountain
- How were we going to ensure business continuity if both data centers were destroyed!
- Diversifying is critical and essential

HOW TO PLAN

- Diversity is key to IT, just as it is with investments
- You don't keep all your eggs on one basket
- https://www.ready.gov/business/implementation/IT
- Test with outside groups
- If you have an emergency manager, ask them to come up with a scenario
- You will be shocked how well this may work

TEST YOUR PLANS

- Once plans have been made – test them!
- Disaster planning is only good if it works
- Plan for the worst
- Diversify
- Partner with other entities

CONCLUSION

- Understanding what could happen is the first step
- Plans can be designed to account for everything, but at what cost?
- Planning and testing go hand in hand

IF YOU BUILD IT – THEY WILL GET AROUND IT

OBJECTIVES

- Understand how undue burdens on employees cause more harm than good
- Discuss how to listen to your audience
- Explore how IT departments can be a partner with stakeholders

A HARD JOB

- Information technology departments have a hard job
- It's not only a balance of keeping the customers happy while implementing new technology, it's a balance of implementing the right technology at the right time with security in mind!

CASE STUDY: NAC

- NAC stands for network access control
- Several years ago, the university had a network access control product that would check your system for updates and antivirus
- The system was black and white
- 55% of users decided that they would use the open network and jump on VPN rather than a black and white system

CASE STUDY: NAC - 2

- System was analyzed, feedback was presented
- System was replaced with a better system that wasn't so black/white
- Saw decrease from 55% on unsecured network to less than 10%
- Partnering with your stakeholders will allow flexibility

BURDENS

- While IT security is a must these days, we cannot afford to not know what we don't know
- Sometimes putting restrictions on employees have the opposite effect – they will hide from you or bypass security
- Corporate data needs to be protected, however partnering with employees and coming up with an equitable solution will not put undue burden on users

DO'S AND DON'TS OF SYSTEM SUPPORT

- Do:
  - Partner with employees and stakeholders for solutions
  - Come up with a sustainable model for security
  - Understand users don't understand systems the way you do
  - Be transparent
  - Put a logical plan in place
- Don't:
  - Release software without proper releases and support
  - Release services without proper documentation
  - Release security software that hurts the greater good

PARTNERING WITH STAKEHOLDERS

- Stakeholders are any one that is invested in a system
- This could be many different people
  - In a university this could be students, faculty, staff, executives, system owners, system support
- Hold regular meetings
- Come up with plans to include them in conversations and decisions
- Explore effective change management

CONCLUSION

- Users need support from IT staff
- IT needs to in turn listen
- If you build something that the users hate, you have done a disservice to your service organization

UPGRADING ENTERPRISE SYSTEMS

OBJECTIVES

- Understand need for upgrading enterprise systems
- Discuss strategies for upgrading systems
- Discuss change management

UPGRADING ENTERPRISE SYSTEMS

- Enterprise systems are systems designed to be used throughout the enterprise
- These could include services that are offered
  - Mail
  - DNS
  - Web servers
  - Video streaming
  - ERP systems

WHY UPGRADE?

- Security vulnerabilities
- Functionality
- Stability issues
- Systems get old

UPGRADE STRATEGIES

- There are many upgrade strategies out there
- Software typically comes with automatic updates however patching software is not always straight forward
- Careful analysis needs to be performed on systems to understand impact
- Package managers, especially for Linux systems allow safe upgrade paths, however dangers still remain
- Hardware becomes more difficult and may be prone to failure

CHANGE MANAGEMENT

- Optimize overall business risk
  - It is often correct to minimize business risk, but sometimes it is appropriate to knowingly accept a risk because of the potential benefit
- Changes should be managed to:
  - Optimize risk exposure (supporting the risk profile required by the business)
  - Minimize the severity of any impact and disruption
  - Achieve success at the first attempt
  - Ensure that all stakeholders receive appropriate and timely communication about change so that they are aware and ready to adopt and support the change

DEFINITION OF CHANGE

- The addition, modification or removal of anything that could have an effect on IT services in production. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

EFFECTIVE CHANGE MANAGEMENT

- Risks are taken into account
- Timelines are reviewed
- Backout plans established
- Stakeholders meet to discuss
- Post implementation discussed

CONCLUSION

- Upgrading equipment and software is essential for any enterprise or organization
- Planning is the key to successful change

WHEN SOMETHING GOES WRONG

OBJECTIVES

- Explore incident response plans
- Understand how organizations rely on people to support them
- Discuss what to do during an incident

SOMETHING WILL ALWAYS GO WRONG!

- Something will always happen, we talked about this before in “Planning for Disaster!”
- How we deal with various incidents or outages should be defined

WHAT IS AN INCIDENT?

- Incident
  - Whenever a user is not receiving an expected level of service from an IT service. Expected levels of service are based on Service Level Agreements (SLA).
- Major Incident/Outage
  - A major incident is defined as a significant event, which demands a response beyond the routine, resulting from uncontrolled developments in the course of the operation of any establishment or transient work activity.

INCIDENT RESPONSE PLANS

- According to SANS incident response plans should include:
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- The goal is to minimize damage
- This could be a course on its own!

UNDERSTAND YOUR CRITICAL SYSTEMS

- Identify your mission critical systems
- Identify support services for those systems
- For Example:
  - Network – Firewalls, Switches, Routing, Connections to data centers, Connections to mission critical buildings
  - Power disruptions – Data center outages

DEFINE YOUR ROLES

- Understand who is in charge and who will do what

COMMUNICATE!

- Communication is tough, especially in an emergency
- Define who should have the communication role and who to send notifications to

IDENTIFY LOGISTICS

- If a major outage occurs:
  - Who gets sleep and when?
  - Who runs and gets food?
  - Who has a company credit card on them at all times?
  - What about after the incident?

CONCLUSION

- Incident response plans are essential to survive an outage or incident
- Defining and practicing will get you far

BASELINING AND ASSESSMENT

OBJECTIVES

- Understand how we know that systems are performing as they should
- Explore effective baselining
- Discuss performance and load testing