Understanding Vulnerabilities and Security Risks

Module Overview

Cloud-based vs. on-premises

Zero-day vulnerabilities

Weak configurations

Third-party risks

Patch management

Legacy platforms

Impacts

Cloud-based vs. On-premise

Cloud-based

Cons:

Larger attack surface and multi-tenant infrastructure

Less direct control over security as it’s managed by 3rd-party and/or contractors

Pros:

Large security team constantly monitoring

Typically larger investments in people, process and technology

On-premises

Cons:

Constant need to refresh and maintain infrastructure

Patching, upgrade firmware, monitor for security issues

Pros:

Direct control over security

Single-tenant infrastructure (usually) with dedicated security team

New Threats/Zero Day

Government / Nation States

Organized Crime / Hacking Groups

Hacktivists / Script Kiddies

Sophisticated / expensive → Unsophisticated / inexpensive

Misconfiguration / Weak Configuration

Weak or improper configurations can expose an organization to risk

- False sense of security
- Gaping holes in defenses
- Increase the attack surface

Mitigated through vulnerability scanning and security audits

- Establish a security/configuration baseline for each system and periodically audit

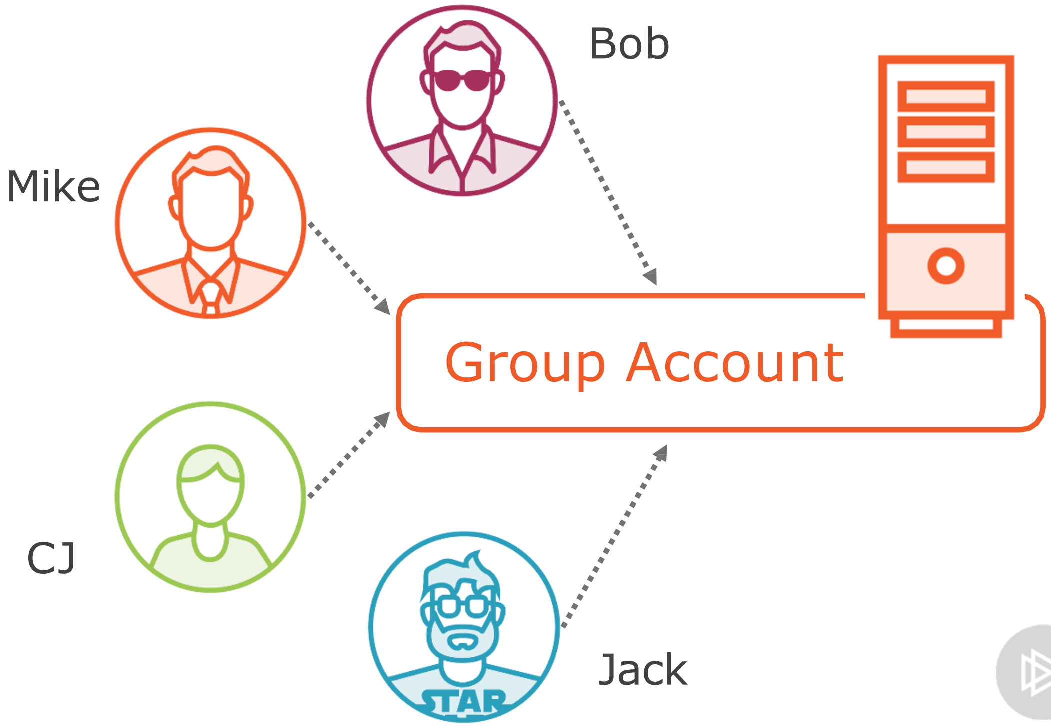
Shared Accounts (Improperly Configured)

Users should not be able to share accounts / group accounts

- Reduces auditing/logging
  - Very hard or impossible to tell what user(s) made a change, accessed or deleted a file, etc.

Non-repudiation

- Being able identify and validate user activity



Weak Configuration Considerations

Open permissions

Unsecured root accounts

Errors (how they are handled)

Unsecure protocols

Default settings

Open ports and services

Weak Cipher Suites and Implementations

Cryptographic algorithms used in a connection are bundled together to form cipher suite. Each suite contains:

- Key exchange
- Authentication
- Encryption
- Integrity algorithm

All four algorithms are not used all the time, depending on what is needed

Weak Cipher Suites and Implementations

The following encryption algorithms should not be used:

- RC4
- Triple-DES
- ‘NULL’

Industry best practices is to not use Triple-DES and use AES-128 or AES-256 instead

Improper Certificate and Key Management

Many companies are at risk due to poor certificate and key management practices

- Manual certificate/key management
- Lack of insight / reporting automation
- No centralized policies
- No method to replace compromised CA certificates

Secure Protocols

When given the option, always choose the highest security possible when establishing communications over an unsecure medium

- FTPS
- HTTPS
- SSL/TLS
- Secure POP/IMAP

Default Configuration

Default configurations shouldn’t be considered secure

- Change things like admin accounts, default passwords
- Harden systems wherever possible
- Establish baselines and periodically audit for compliance

Establish a patching and lifecycle management cadence

Third-Party Risks

Vendor management

- System integrations
- Lack of vendor support

Supply chain

Outsourced code development

Data storage

Vendor management

- Do their systems integrate with yours?
- Are they acquiring new systems or deprecating existing ones?
- Can/will they force you to upgrade or buy new?

Mergers/acquisitions

- Do existing vendors support the newly acquired systems

Lack of vendor support

Vulnerable Business Processes

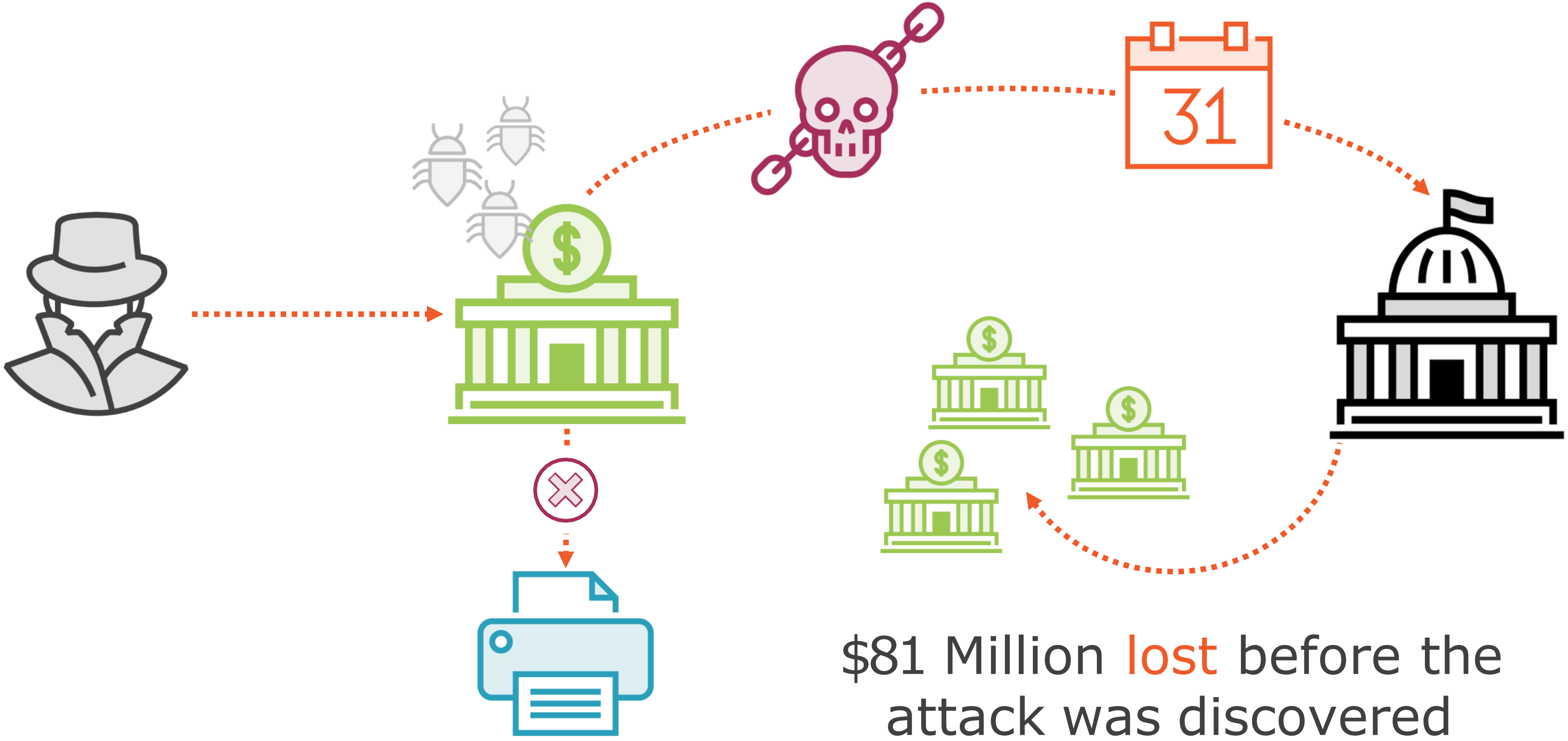
Business Process Compromise (BPC)

- Targets the unique processes or the systems facilitating those processes to covertly manipulate them; typically for financial gain

Once a foothold is gained within an enterprise, attackers move laterally and quietly study systems and processes over time

- Intimate knowledge of processes is developed to make detection difficult
- Can disrupt internal processes or a target's interaction with outside/3rd party systems

Business Process Compromise (BPC)



$81 Million lost before the attack was discovered

Outsourced Code Management

Agreements in place

- Are there operating agreements stating who owns the code?
- How are liability and potential damages addressed?
- Where is data stored, how is it secured?

Improper or Weak Patch Management

Firmware
Firmware on things like NICs, HBAs, disk drives, graphics cards, etc., can create compatibility issues when other things are updated if not in sync

Operating Systems (OS)
Vulnerabilities are constantly being discovered, and one of the best defenses is to keep systems patched and up-to-date

Applications
Applications, OS and firmware/drivers should be kept in sync as much as possible (refer to hardware compatibility matrix) for most systems

Legacy Platforms

Security vulnerabilities
Older platforms often have bugs/vulnerabilities that don’t have patches or updates readily available

Hardware failures
As infrastructure ages, the rate of failures increase and the availability of parts decreases – introducing risk into the environment

Tribal knowledge
Older platforms may have fewer people who are subject matter experts, making administrating and maintaining more of a challenge

Impact Areas

- Data Loss
- Data Breaches
- Data Exfiltration
- Identity Theft
- Availability Loss

Effects of Impacts

Financial Impact

Reputation Impact

Module Review

Cloud-based vs. on-premises

Zero-day vulnerabilities

Weak configurations

Third-party risks

Patch management

Legacy platforms

Impacts