AAPA 2017 Executive Management Conference May 2, 2017

Information Technology — Enhancing Productivity
and
Securing Against Cyber Attacks

AGENDA

- Brief Overview of PortMiami
- Enhancing Productivity Using Technology
- Technology Being Using at the Port
- Cyber Attacks
- Securing Systems
- Questions

- PortMiami is Miami-Dade County's second most important economic engine, contributing $41.4 billion annually to the local economy and supporting more than 324,352 jobs in South Florida.
- Recognized as the Global Gateway.
- Miami's unique geographic position makes the Port easily accessible to Caribbean and Latin American markets, as well as those of Asia and Europe by way of the Panama Canel.


PORTMIAMI
CRUISE
Total Cruise Ships Docked 972
Cruise Passengers 4,980,490
Cruise Lines 18
Cruise Ships 42
CRUISE
Known worldwide as the "Cruise Capital of the World" PortMiami is the global headquarters for five leading cruise lines.


PORTMIAMI
CARGO
Total Cargo Ships Docked.....1,081
Total TEUs 1,028,156
Total Tonnage 8,777,974
CARGO
A new era is here and PortMiami is ready! Capital improvements in excess of $1 billion are now complete.
PortMiami is ready for the new generation of containerized cargo. We are Big Ship Ready!

Enhancing Productivity Using Technology

Business Productivity

- Using technology to maximize your business productivity creates the platform to realize true business success.

- Increased business productivity can be traced to the automation of processes allowing for:
  - faster communication of strategy
  - increased time spent on strategic priority
  - greater project completion rates.

Improving Efficiency

- Technology can help you improve the way your staff carry out tasks.
- This can either speed up existing processes or allow new, more flexible ways of carrying out the job.
- In order to work out the best technology for your needs, you should assess your current systems against your requirements.

Improving Efficiency

- Think about how you can:
  - ✓ Capture relevant information in the most simple,time-efficient way.
  - ✓ Manage your documents to ensure that information is dealat with ina logical workflow.
  - ✓ Avoid duplication.
  - ✓ Address technological obstacles.

- The best solution for your business will depend greatly on your industry. Research what your competitors or other companies in your industry are using and consider consumer technologies that are widely available.

Cyber Attacks

What are Cyber Attacks?

- Deliberate exploitation of computer systems, technology-dependent enterprises and networks.

- Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

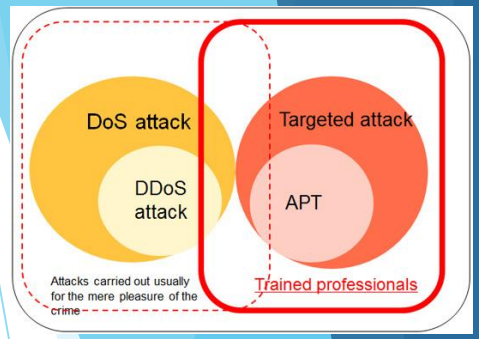

IS YOUR BUSINESS AN
EASY TARGET
FOR CYBER ATTACKS?

The Big Cyber Threats Breakdown: Types of Cyber Attacks

Web Threats

Any threat that uses the Internet to perform some sort of malicious activity.

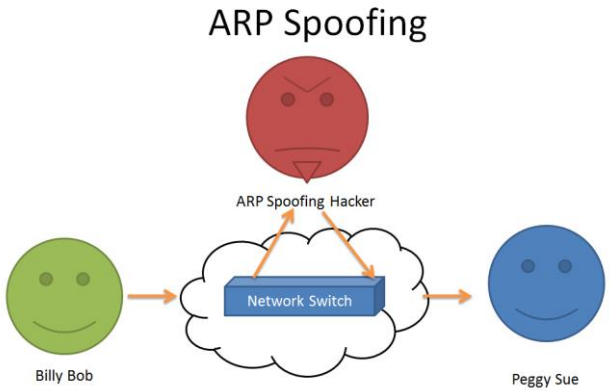
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks



- In a DoS attack, a single attacker directs an attack against a single target, sending packets directly to the target.
- In a Distributed DoS (DDoS) attack, multiple PCs attack a victim simultaneously. A series of computers scan target computers to find weaknesses and then compromise the most vulnerable systems. In a DDoS attack:
  - The attacker identifies one of the computers as the *master* (also known as *zombie master* or *bot herder*).
  - The master uses *zombies*/*bots* (compromised machines) to attack.
  - The master directs the zombies to attack the same target.
  - The attacker is able to effectively hide his identity by being two hops away from the victim.
- A Distributed Reflective Denial of Service (DRDoS) uses an amplification network to increase the severity of the attack. Packets are sent to the amplification network addressed as coming from the target. The amplification network responds back to the target system.

Spoofing

- Used to hide the true source of packets or redirect traffic to another location
- Use modified source and/or destination addresses in packets.
- Can include site spoofing that tricks users into revealing information.
  - IP spoofing changes the IP address information within a packet
  - MAC spoofing is when an attacking device spoofs the MAC address of a valid host currently in the MAC address table of the switch
  - ARP spoofing (also known as ARP *poisoning*) uses spoofed ARP messages to associate a different MAC address with an IP address



Wireless Networks

- A *rogue access point* is any unauthorized access point added to a network. Rogue access points can allow the unauthorized capture of credentials and other sensitive information as well as conduct phishing and man-in-the-middle attacks
- With *wardriving*, an attacker scans an area looking for available wireless networks.
- *Packet sniffing* (also known as *eavesdropping*, *snorting*, or *snarfing*) is the interception and possible decoding of wireless transmissions
- *Interference* is a signal that corrupts or destroys the wireless signal sent by access points and other wireless devices
- Although NFC transmission distances are very short, it is still susceptible to several types of malicious attacks,

Passwords

- Using tools to check for unencrypted or weakly encrypted passwords sent through the network.
- Guessing passwords by trying:
  - Default passwords for new systems, Blank passwords, Use password as the password, Rows of letters on the keyboard (e.g., qwerty), User's name or login name, Name of significant other, Birthdate,
  - Using social engineering to get a user to reveal the password. For example, the attacker can pretend to be an administrator that needs the user's password.
  - Using brute force attacks.
  - Using tools to crack passwords:
- Programs, such as SnadBoy's Revelation, which reveal a hidden password in clear text.
- Keylogging software which can capture a user's screens, clipboard data and visited Web sites in addition to logging keystrokes.

Sophistication of Attacks

- Difficult to distinguish an attack from legitimate traffic.
- Behavior, making the same attack appear differently each time
- Proliferation of attack Software
  - Variety of attack tools available
- Scale & velocity of attacks
  - Attacks grow to millions of computers in a matter of minutes or days

Securing Against Cyberattack

NIST
National Institute of Standards & Technology

- Created through collaboration between industry and government, the Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Protection Against Web Threats

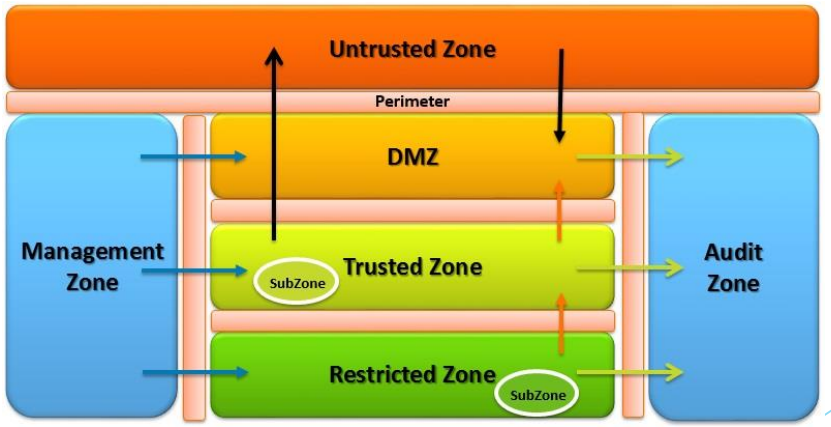
- Web site/URL content filtering
- Web threat filtering
- Gateway E-mail Spam blockers
- Virus blockers
- Anti-phishing software

Prevent Malware Attacks

- Use the latest version and patch level for the Web browser.
- Install the latest patches for the operating system.
- Install antivirus, anti-spyware, anti-rootkit, and personal firewall software. Keep definition files up-to-date.
- Use a pop-up blocker to prevent adware.
- Use software to control cookies on the system.
- Do regular scheduled scans to look for malware.
- Choose anti-malware software from a reputable company. Don't be fooled by scareware into purchasing a product that may not work.

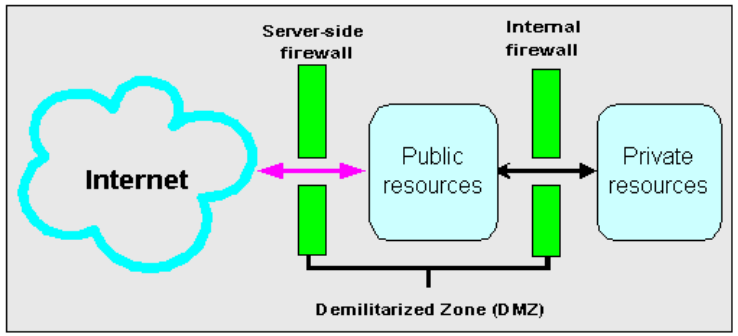
Security Zones

- An *intranet* is a private network (LAN) that employs Internet information services for internal use only
- The Internet is a public network that includes all publicly available Web servers, FTP servers, and other services.
- An *extranet* is a privately-controlled network, distinct from, but located between the Internet and a private LAN
- A *demilitarized zone* (DMZ) is a network that contains publicly accessible resources.



Demilitarized Zone (DMZ)

- Be aware of the following DMZ facts:
  - If the firewall managing traffic into the DMZ fails, only the servers in the DMZ are subject to compromise. The LAN is protected by default.
  - Packet filters on the firewall allow traffic directed to the public resources inside the DMZ. Packet filters also prevent unauthorized traffic from reaching the private network.
  - When designing the firewall packet filters, a common practice is to close all ports, opening only those ports necessary for accessing the public resources inside the DMZ. Typically, firewalls allow traffic originating in the secured internal network into the DMZ and through to the Internet. Traffic that originates in the DMZ (low security area) or the Internet (no security area) should not be allowed access to the intranet (high security area).



Firewalls

- A device or software running on a device that inspects network traffic and allows or blocks traffic based on a set of rules
  - A *network-based* firewall inspects traffic as it flows between networks. For example, you can install a network-based firewall on the edge of your private network that connects to the Internet to protect against attacks from Internet hosts. Network-based firewalls are typically dedicated hardware devices.
  - A *host-based* firewall inspects traffic received by a host. Use a host-based firewall to protect against attacks when there is no network-based firewall, such as when you connect to the Internet from a public location.

Additional Network Security Solutions

- A *proxy server* is a type of firewall that stands as an intermediary between clients requesting resources from other servers
- An Internet *content filter* is software used to monitor and restrict content delivered across the Web to an end user
- Network Access Control (NAC) controls access to the network by not allowing computers to access network resources unless they meet certain predefined security requirements
- All-in-one security appliances combine many security functions into a single device
- An *application-aware* device has the ability to analyze and manage network traffic based on the application-layer protocol that created it

Penetration Testing

- The attempt by an organization to circumvent security controls to identify vulnerabilities in their information systems
  - Verifying that a threat exists
  - Bypassing security controls
  - Actively testing security controls
  - Exploiting vulnerabilities

Security Management

- The overall security vision for an organization and the ongoing implementation and maintenance of security. Its goal is the preservation of the confidentiality, integrity, and availability of all critical and valuable assets
  - Assess the risk
  - Create a policy
  - Implement the policy
  - Train the organization on the policy
  - Audit the plan to make sure it is working

A Security *Policy*

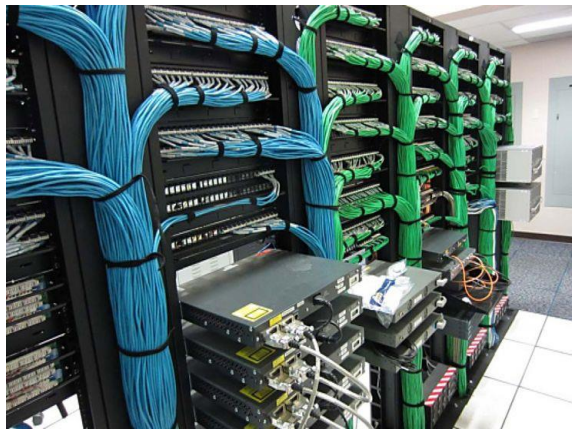
- Defines the overall security outlook for an organization. To be effective, the security policy must be
  - Planned. Good security is the result of good planning.
  - Maintained. A good security plan must be constantly evaluated and modified as needs change.
  - Used. The most common failure of a security policy is the lack of user awareness. The most effective way of improving security is through user awareness.

Risk Management

- The process of identifying vulnerabilities and threats and deciding what countermeasures to take to reduce risks to an acceptable level
- The main objective is to reduce the risk for an organization to a level that is deemed acceptable by senior management

Manageable Network Plan

- Process created by the National Security Agency (NSA) to assist in making a network manageable, more defensible, and more secure
- The plan identifies a series of milestones for creating a manageable network plan, offers suggestions, gives crucial security tips, and provides references



Employee Management

- Implementation of processes to ensure that employees play a major role in protecting company assets
- Three important principles that should be part of every employee management decision are:
  - The principle of *least privilege* specifies that an employee is granted the minimum privileges required to perform duties of the position.
  - The principle of *separation of duties* specifies that for any task in which vulnerabilities exist, steps within the tasks are assigned to different positions with different management.
  - The principle of *two-man control* specifies that certain tasks should be dual-custody in nature to prevent a security breach.

Employment Agreements

- Documents that explicitly identify the terms and conditions of employment
  - Non-disclosure agreement (NDA)
  - Non-compete agreement
  - Ownership of materials agreement
  - Data handling and classification policy
  - Clean desk policy
  - Acceptable use agreement
  - Password security policy
  - Employee monitoring agreement
  - Exit interview cooperation agreement

Questions & Open Discussion

Michelle R. Thames