To: Business and Finance

From: Security and Network Services

Date: 12/15/08

RE: Virtualization as a Service Security Strategy

Purpose

The goal is to provide seamless and effective security for customers of Virtualization as a Service without impact to their business requirements. These measures should provide security across all components of the architecture and should include but not be limited to storage, networking and application security procedures.

Though network security is a priority to this project and effort is made to screen the VaaS components from other MAIS provided services, network perimeter security it is not required by the customer to participate. The intent is to provide a virtual machine hosting service that allows a VaaS customer to use any network and security infrastructure that they have currently in place, or to participate in any security services provided centrally on campus by technologies such as the Virtual Firewall.

Objectives

The extent of the security measures should provide the maximum level of security without impacting a VaaS customer’s business requirements. The final solution should be adaptable to new security technologies while providing flexibility to the VaaS customer. Key features will include:

- A network segment for each VaaS host that corresponds with its organizational boundary at the virtual and physical switch layers and does not prevent the use of a network security device such as a firewall where requested by the VaaS customer. Since this device would not be provided as part of VaaS, it would need to be supported either by the VaaS customer, or a member of a central IT Security group such as ITSS.

- Monitoring bandwidth usage for each of the VaaS customers to track potential bandwidth exhaustion and discover compromised hosts.

- Communication to the administrators of the VaaS virtual machines the importance of following secure administration procedures.

- Authentication, authorization and auditing of VaaS administrator’s access to the central VaaS console that will provide appropriate levels of access to VaaS customers and track both successful and unsuccessful connection attempts.
General Policy

Bandwidth monitoring
Netflow, a tool used to illustrate network traffic patterns will be used to capture packet information such as source, destination and payload size. Additionally, the Virtual host will be configured to monitor and alert on bandwidth thresholds of both the virtual machines and virtual host.

Packet filtering
In the event that a stateful inspection firewall cannot be deployed, an Access Control List will be developed to broadly isolate the VaaS service from non-VaaS hosts on the same physical switch.

Virtual Switch segmentation
All VaaS customers will be restricted to a single Virtual Switch that processes traffic for the VaaS service only. It does not see traffic destined for non-VaaS networks.

Network segmentation
Routed network space will be allocated to each unit and will be filtered by an access list on the physical switch or a perimeter security device. VLANs will be assigned to the routed network space on the physical switch. On the virtual host, port groups that represent these VLANs will be configured to separate these network spaces. All network cables connected to the VaaS Virtual Switch will be assigned to networks of the VaaS service customers only.

Application Security
The VaaS administrators will follow patch procedures for the virtual machine hosts in keeping with MAIS patching standards. This includes applying patches that fall into a category of Critical within 36 hours of their release.

The VaaS infrastructure console, where accessible by VaaS customers will provide appropriate access control and will log all connections and connection attempts. The integration with the MPATHWAYS Active Directory Domain provides both authentication and authorization services for VaaS.

The Infrastructure console has also been strategically placed on the Citrix farm to prevent opening up access directly to campus.

Storage Security
Disk storage assigned to VaaS customers is hard zoned and available to the interfaces installed on the virtual hosts dedicated to VaaS only.

Responsibilities
VaaS customers should be aware of the security principals involved in providing host level security which includes but is not limited to:

- Removing unnecessary processes and accounts
- Installing and configuring Anti-Virus software to automatically update
- Installing and configuring a local firewall
Applying critical patches promptly. Critical patches for both Operating Systems and applications should be applied as soon as possible.

Sanitizing disk assigned to them when no longer required. VaaS customers will be responsible for sanitizing vdisks assigned to them if they choose not to participate in the VaaS service, or when retiring particular VaaS hosts assigned to them.

MAIS Security staff under the direction of the ISSO will be responsible for monitoring VaaS customers for exceeding bandwidth and ensuring that network segments are created and appropriately sized.

MAIS virtualization staff will be responsible for maintaining the virtual switch within the Virtual Host configuration and ensuring that hosts are properly allocated to the appropriate network segment and that access to those hosts are only granted to the corresponding VaaS customer. They will also be responsible for ensuring that the virtual machine hosts are hardened and properly patched and have appropriate local packet filtering and access controls.

MAIS management and virtualization staff will be responsible for communicating the impact of a VaaS customer that exceeds assigned bandwidth thresholds or whose host is suspected of being either compromised, or of attacking other VaaS or MAIS hosts via the network. This communication will be via the Service Level Agreement and will include information on the circumstances and actions to be taken by MAIS staff during such an event.

**Glossary**

**ISSO:** Information Systems Security Officer

**VaaS:** Virtualization as a Service

**VLAN:** Virtual Local Area Network