ISSP-015 - Server Address Assignment and ACL Requests

INTRO

In order to improve the security posture of the servers part of the IT SVC Data Center and Winter Haven Data Center, the IT’s Office of Information Security, in conjunction with Communications Infrastructure and the Data Center Infrastructure group have established a set of network procedures to be followed when setting up a server.

SCOPE

This document addresses all servers being consolidated and new servers being purchased and set up in the SVC Data Center and Winter Haven Data Center.

SEGMENTED NETWORK

Two groups of 4 subnets have been set aside for IT servers. One group is reserved for the primary data center (SVC) and the other for the secondary data center at Winter Haven. Within each group, there are 4 levels of security. Determination of a new server’s appropriate tier will be performed on each individual case by the functional user and IT personnel.

SECURITY LEVELS

The four security levels are:

Level 0 - Extremely restricted access

This level should be used for any server which hosts restricted personal data, as defined on ISSP-001, Sensitivity and Criticality of Data. Examples of this data type include but are not restricted to credit card information, student records, etc. Access to machines in this network should be limited to select application servers and as few desktops as possible. Access should be granted on a per-IP and port basis. No off-campus access should be permitted from these hosts (not even for updates). Exceptions are made due to regulatory compliance, on a case-by-case basis.

Level 1 - On-campus only access.

Servers in this level should be restricted to on-campus access only for inbound connections and only those IP's/Ports which are minimally required should be permitted to the server's IP. Outbound traffic can be permitted if necessary, but should be restricted to the protocols which are required. For example, traffic required for OS/application updates should be limited to only the protocols (FTP, HTTP/HTTPS, etc) that are required and preferentially these updates should be hosted on campus so that the machines at this level do not require any off-campus outbound access.

Level 2 - Public Servers.

This level should be used for servers which host public resources (web servers, etc). Inbound access should be restricted to only those ports which are necessary for the hosted application. Outbound traffic
should be restricted to only those protocols which are required for the application or for OS/application updates.

Level 3 - Hosted Servers.

This level is reserved for machines which aren't under the direct control of IT. For example, servers which are housed in one of the data centers for other USF organizations should be placed in this level. Inbound and outbound access should be restricted to only the required protocols.

ADDITIONAL TIERS

Infrastructure

Network for infrastructure devices (KVMs, DRAC, iLO, etc). This network is reserved for any infrastructure devices which should not have public access.

HIPAA

The HIPAA network within the SVC Data Center is still to be determined. There is no HIPAA data within the Data Center at this point.

ACCESS CONTROL LISTs

ACls are key to the establishment of the separate network tiers. Servers placed in the tiered network must be profiled prior to setup in order to determine the level of access required. Functional users will work with Data Center Infrastructure group to make that determination.

Once the level of access and profile is determined, an email will be sent to

acl_request@lists.acomp.usf.edu

with detailed information about the access required and a description of the new server being setup. The following is an example of a proper request:

<table>
<thead>
<tr>
<th>Source:</th>
<th>Hotei.fastmail.usf.edu (131.247.89.15)</th>
<th>USF IT App Server Dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination:</td>
<td>USFCas1.forest.usf.edu (131.247.80.161)</td>
<td>USF CAS mail servers</td>
</tr>
<tr>
<td></td>
<td>USFCas2.forest.usf.edu (131.247.80.162)</td>
<td></td>
</tr>
<tr>
<td>Port(s):</td>
<td>80 (TCP), 443 (TCP)</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Description:</td>
<td>Application account needs access mail hub servers</td>
<td></td>
</tr>
</tbody>
</table>