TO: Philip Carson

FROM: IT Staff

Subject: 044 – Final System State Report

# State of Security

## System Updates

All Linux machines were updated with the latest available packages by using the update manager. A cron job was installed to retrieve and install the latest updates on a weekly basis. The Windows based machines were configured to use windows update services (WSUS) to automatically provide updates.

## Password Changes

All passwords were changed to more secure versions that should be extremely difficult to crack.

## User Audit

All systems have been audited to identify active users. User accounts corresponding to terminated employees have been deactivated. Industry standard security tools have been used to verify the strength of all user passwords on all UNIX systems. The same task still needs to be done on the Windows related machines.

## Shutdown Non-essential Processes/Services

All machines have been audited to determine what services are running. Non-essential services such as the Cups printing daemon, HP Service and Status daemon, Portmapper, RPC statd, IIS, etc... were identified and shutdown. These services are not needed to fulfill the business requirements and represent vulnerability risks to the system.

## Application Security Updates

Administrator users to the web interface have had their passwords changed to more secure passwords. The web application is running using a content management system called Drupal. This system uses the PHP scripting language. The PHP configuration was modified to prevent scripting attacks. Further analysis of the application is required to check for industry standard security best practices. Newer versions of the application may be available that fix potential security vulnerabilities. This will be part of our recommendation to further secure the system which will be outlined later. This is a complex task and needs to be planned carefully to ensure that there is no interruption to Maestro Games’ core business.

## Security Vulnerability Scanners and IDS

Industry standard security scanners have been run on the system and potential vulnerabilities have been identified, particular on our DNS server. We made it a priority to analyze and patch this particular system based on this action. We also identified particular IP addresses that were performing denial-of-service attacks on our web server via these systems. Such IP addresses were then blacklisted to ensure that they do not interrupt the core business of Maestro Games.

## System Level Audits

We performed various audits on all systems. Refer to the changelogs for details.

## Reconfigure Internal Services

Some services were configured to listen on all interfaces, which makes the services exposed than they should be. These services were reconfigured to listen only on internal interfaces. In the case of the web server, there is an instance of MySQL co-located on the same machine. To lock down the MySQL server and prevent access from outside users, we configured this instance of MySQL to listen only on the localhost interface.

# Security Recommendations

## Application Code Review

We are recommending that the Drupal content management be reviewed for compliance with industry standard security practices. This includes the use of proper input validation and configuration. Multiple vulnerabilities in the current Drupal install have brought the website down throughout the day. Patching or updating Drupal should resolve these issues, but it may be necessary to switch to a new content management service. We estimate this task could take up to 120 man hours at 100 dollars an hour resulting in a 12,000 dollar cost. This maximum would include experienced people auditing and reviewing the code to guarantee security.

## Redundant Services

To ensure that we can always maintain the states of company services, it is necessary to back them up. We request that we backup both the DNS server and the Web server. This would allow us to maintain DNS support regardless of if the DNS server is attacked. Furthermore backing up the Web Server would allow for both load-sharing to prevent DoS attacks and provide backups for if one of the two servers is taken down. This would require a maximum of $4,000 dollars for both servers and $9,000 dollars for each server. This would take around 3 weeks for planning implementation and testing.