Client Assessment

High Level Information Technology Assessment

Thursday September 7, 2010

Introduction

Thank you for the opportunity to provide [redacted] with a courtesy assessment of the current Information Technology (IT) environment and provide recommendations that support [redacted] future IT goals.

This document provides a high-level view of the computing resources in use at [redacted], focusing on security, the network, the server environment, the backup environment, and the primary / business critical applications.

As a part of our assessment, we evaluated the current configuration and compared it to industry standard best practices.

What is an IT Assessment?

As different company environments can range from fairly straight forward and simple to highly complex, we take a look at a five key areas. A description of each area included in the assessment is described below:

1. **Security Environment**

   We want to understand what security measures are in place or lacking to protect [redacted] from both internal and external access to unauthorized areas of the IT environment. Here we take a look at areas like physical access to the servers, password policies, admin rights, Antivirus, critical updates, SSL certificates, etc.

2. **Network Environment**

   We want to understand Alameda Dental Group's topology. We look at your: LAN – how this office desktops and servers communicate; WAN – how this office communicates with another office and how this office communicates with the Internet; VPN – how remote users (i.e. laptop road warriors) communicate with this office.

3. **Server Environment**

   This is the heart of your computing infrastructure. In addition to the basics (CPU, RAM, OS, Disk capacity, etc.), we look for different information depending on the role of the server – Domain Controller, File & Print, Exchange, etc.

4. **Backup Environment**

   This typically falls under the server arena. However, we believe that backups are so vitally important that we break it out separately. We look to see if backups are being performed, the version of the backup software, offsite storage, media, etc.

5. Primary/Business critical applications

We want to understand the technical configurations around your critical applications. This includes items such as redundancy, performance, security, etc.

Findings

The findings have been categorized into four severity levels. These severity levels are defined as: Critical - Critical findings are issues that C3 Solutions feels should be addressed immediately to prevent the high likelihood of an interruption of service or loss of data. Important - Important findings are issues that are causing a problem are a potential problem and should be addressed as soon as possible. Theses issues are affecting performance. Best Practices – Are defined by the vendor to maximize the feature set of the software. Informational – This category is for your information only. Each item will be preceded by the appropriate severity.

1. Security Environment

a. Critical – Access to email via Outlook Web Access or OWA is currently using http or clear text. An SSL certificate is needed to protect and encrypt the contents of email. This is a HIPAA issue.
b. Critical – On NAS 3 all users have rights to everyone's my documents directory, journal entries, and the common directory which contains patient information. This is a HIPAA issue.
c. Critical – All users have access to the common directory on NAS 2 which contains patient information. This is a HIPAA issue.
d. Critical – There is currently no logging enabled for NAS 2 and NAS 3. Auditing is a HIPAA requirement and should be enabled and reviewed. There should be policy outlining this review process.
e. Critical – NAS 2 and NAS 3 do not have the latest Microsoft security updates. NAS 2 does not have the latest anti-virus signatures.
f. Critical – The current password policy is not strong enough to successfully pass a HIPAA audit. Most users' passwords are set to never expire which overrides the password policy. This is a HIPAA issue.
g. Important – The Sonicwall firewall is not monitored. This device should be monitored in real-time to ensure security. This is a HIPAA issue
h. Important – The anti-virus real time protection has been disabled on both NAS 2 and NAS 3. Because users are saving files on these servers this feature should be enabled.
i. Best Practices – The Sonicwall firewall contains rules for a device with an IP of 192.168.1.220 which no longer exists or is turned off. If these rules are no longer needed they should be disabled or deleted.

2. Network Environment

a. Informational – Remote access is available via VPN and or Terminal Services. In addition email is available via OWA or RPC over HTTP. All of these features do not appear to be implemented. There are benefits to utilizing these features.
b. Informational – The firmware on the Sonicwall is not up to date.

3. Server Environment

a. Critical – Many servers had a message that they were shut down unexpectedly when they were accessed by C3 Solutions. This indicates a problem that could lead to operating system corruption which can cause significant downtime.
b. Critical – One of the two hard drives in ADGPDC is in a failed state. This leaves Almeda Dental exposed because this server is operating on one drive and is the only domain controller for the domain. There should be a second domain controller on the network for redundancy.
c. Important – Both NAS 2 and NAS 3 have only 9 GB available which is only 6% of total capacity. Operating at this capacity causes performance degradation. Backups make up ~ 60GB of data on these servers. This can be eliminated with the proper configuration.
d. Important – NAS 2 is very fragmented. This will cause poor performance. This should be setup to run automatically and monitored by monitoring software.
e. Important – Unauthorized software is installed on DBServer. This software is called Bit Lord and is used to obtain software illegally from shared sources on the internet.
f. Important – Cane is currently running at maximum memory capacity. At least 1GB of memory should be added to Cane to ensure proper functionality.
g. Best Practices - DNS is currently running on PAUL which is not a domain controller. DNS is configured as an Active Directory Integrated Zone and should only be on a domain controller. DNS should have been moved when PAUL was demoted from the DC role. In addition to pointing to internal DNS servers, servers are also pointing to external DNS servers. Servers should only point to internal DNS servers and the DNS server should forward external requests to the external DNS servers.
h. Best Practices – NAS 2 and NAS 3 are running Computer Associates ETrust Anti-virus. This is different from every other server and therefore has to be managed independently from the other servers. All servers should have the same anti-virus.
i. Informational – Exchange server and Active Directory are running in Mixed Mode. Running in Mixed Mode reduces functionality to ensure compatibility with earlier versions. [redacted] is not running any earlier versions.
j. Informational – RPC over HTTP is not configured. This is a feature of Exchange 2003 which allows users to access their email remotely using the Outlook client without the use of a VPN. This is secured using SSL.
k. Informational – All servers and workstations are downloading and installing updates independently from Microsoft. Windows Update Services should be installed and configured to centrally manage all patch updates.

l. Informational – ADGPDC is indicating that Windows Server and Exchange Server are out of licensing.

4. Backup Environment

a. Critical – The Exchange server, Cane, has transaction logs dated back to February, 2007, which indicates that you have not had a successful full backup of Exchange in nine months. In addition to Exchange there are no backups running on the systems.

5. Primary/Business critical applications

a. Critical – After the migration Mogo looks to be unstable. This appears to be server and or operating system issues.
b. Critical – How is Mogo getting backed up?

Next Steps

Our report has identified a number of areas we believe warrant attention. Our philosophy is to partner with our clients to develop remediation plans that run congruent to their unique priorities and budgetary constraints.

C3 Solutions is capable of helping [redacted] with all areas addressed in this report.