Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementation of a Comprehensive Enterprise Virus Defense Infrastructure in a Global Company

This paper will follow a global corporation's move from traditional, client based and controlled virus defense to a centrally controlled and monitored system. Following the Defense In Depth strategy, the company also augments this new system with policies and procedures to help ensure adequate defense. The evolution of viruses and the speed at which data is now shared globally have brought a new level of threat to the business world. Traditional virus defense initiatives, those that are client based without centralized...

Copyright SANS Institute
Author Retains Full Rights

AD

Implementation of a Comprehensive Enterprise Virus Defense Infrastructure in a Global Company

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 2 - Case Study in
Information Security

Submitted by: Robert Doeden
Security Analyst
Submitted 11/28/04
Class Location: Monterey, CA - 2004

The evolution of viruses and the speed at which data is now shared globally have brought a new level of threat to the business world. Traditional virus defense initiatives, those that are client based without centralized control, monitoring or reporting, no longer make the grade.

This paper will follow a global corporation's move from traditional, client based and controlled virus defense to a centrally controlled and monitored system. Following the Defense In Depth strategy, the company also augments this new system with policies and procedures to help ensure adequate defense.

© SANS Institute 2005, Author retains full rights.

Table of Contents

Abstract/Summary 1
The Company 2
The Corporation: 2
Technology: 2
In the Beginning 3
Security Posture 3
Systems: 3
Processes and Procedures: 3
Problem Description 4
Current Risks 5
Impact of Industry Security Standards on the Situation 5
The Construction of a Fortress 6
Proposed Solution 6
Solution Implementation 9
Implement a centrally managed and monitored virus defense system (ePO) 10
Implement an inline virus defense appliance to scan SMTP traffic initially, HTTP, FTP and POP3 traffic eventually 14
Implement appropriate use policies and institute guidelines and end user education 14
Place virus defense on every computer that can run it that is attached to the LAN/WAN, with minimum 95% compliance. 15
Ensure that 90% or more of the clients report 1 DAT or Engine version old or newer (Current minus 1 or newer) 15
After 16
Solution Testing and Validation 17
Risk Assessment 18
Conclusion 18
References 1
Appendix 2
Security Matrix – Old 2
Overall Security Assessment 2
Assessment by Technology Risk Area 2
Security Matrix –Recent 2
The New Security Matrix Key 2
Overall Security Assessment 2
Assessment by Technology Risk Area 2
Assessment by Attack Vector 2
ePolicy Orchestrator System Layout 2
Original 2
Recent 2
How do I protect my system from computer viruses: 3
What do I do if I receive word of a virus or warning by e-mail? 3
What can you do to help prevent security incidents? 4

© SANS Institute 2005 Author retains full rights.

Camelot Computing Security & Acceptable Use Policy 5
1.0 Purpose 5
2.0 Scope 5
3.0 Policy 5
Charts and Graphs: 9

List of Figures

Figure 1 – Windows O.S. dispersal snapshot for Camelot in 2001 and 2004 2
Figure 2 – Cost of virus defense efforts over 1 year in 2001 4
Figure 3 – Cost of virus defense efforts over 1 year in 2004 16
Figure 4 – Old Security Matrix – Overall Security Assessment 1
Figure 5 – Old Security Matrix – Security Assessment By Technology Risk Area Chart 1 2
Figure 6 – Old Security Matrix – Security Assessment By Technology Risk Area Chart 2 3
Figure 7 – Old Security Matrix – Security Assessment By Technology Risk Area Chart 3 4
Figure 8 – Old Security Matrix – Security Assessment By Technology Risk Area Chart 4 5
Figure 9 - New Security Matrix – Chart Key 6
Figure 10 - New Security Matrix - Overall Security Assessment 7
Figure 11 - New Security Matrix – Security Assessment by Technology Risk Area 8
Figure 12 - New Security Matrix - Security Assessment by Technology Risk Area 9
Figure 13 - New Security matrix - Assessment by Attack Vector 10
Figure 14 - Old ePO System Flow 11
Figure 15 - New ePO System Flow 12

© SANS Institute 2005 Author retains full rights.

Robert Doeden

Abstract/Summary

The evolution of viruses and the speed at which data is now shared globally have brought a new level of threat to the business world. Traditional virus defense initiatives, those that are client based without centralized control, monitoring or reporting, no longer make the grade.

This paper will follow a global corporation's move from traditional, client based and controlled virus defense to a centrally controlled and monitored system. Following the Defense-In-Depth strategy, the company also augments this new system with policies and procedures to help ensure adequate defense.

The corporation uses multiple steps to move from the old to the new, beginning with I.S. getting buy-in and defined expectations from the corporation. I.S. also implements new tools that provide superior control and functionality, and refine their existing tools to meet the new expectations of the corporation. I.S. also identifies and reacts to the human factor, implementing policies, web page FAQs and best practices, security alerting, and end-user education.

As the paper will demonstrate, the corporation was successful in moving from a system that was inadequate in meeting the company's goals and expectations to a system that exceeded those initial expectations. The implementation of this product also showed an added tangible financial benefit and can be demonstrated to show theoretical repeated financial benefits through savings in resources.

Finally, the paper will look at the steps remaining, problems remaining and the likely future of the corporation's efforts.

Note: In all following pages, unless otherwise noted, all clients are assumed to be running Windows operating systems.

The Word We Know:

> **SANS Institute Internet Storm Center**
> **Since its release, a number of severe security vulnerabilities have been discovered in Windows XP. These vulnerabilities are used by worms and viruses, making it impossible to connect an unsecured, unpatched system to the Internet for any amount of time without risking exposure and infection. Users of new computers are faced with the dilemma of being infected by these worms before being able to download the necessary patches.**[1]

[1] SANS

© SANS Institute 2005 Author retains full rights.

The Company

The Corporation:
A global, scientific (Lab and Production) corporation showing a history of steady growth in sales and staff. The corporate headquarters in Anywhere-Anystate, U.S.A. houses the majority of staff in 3 (4 in 2004) buildings. The company has 8 (10 in 2004) branch offices located in Otherplace-Otherstate, U.S.A, Europe, China, Australia, and Japan.
Technology:
The company primarily uses Microsoft operating systems and office suites, with a minor group of notable exceptions: 1 IBM Mainframe and approximately 10-20 Macintosh computers, and a variety of laboratory computers running a variety of operating systems. The company has high speed Internet and utilizes an Exchange mail system over SMTP.

	2001	Operating Systems	2004	Operating Systems
Total Global Servers	60	NT4 Server	80	2003 Server
Total Global P.C.s	720	NT4 Wrkstn, 9x	1170	XP Pro
Anywhere, U.S. Campus Servers	35	NT4 Server	60	2003 Server
Anywhere, U.S. Campus P.C.s	600	NT4 Wrkstn, 9x	850	XP Pro
Otherplace, U.S. Campus Servers	0		5	2003 Server
Otherplace, U.S. Campus P.C.s	0		140	XP Pro
Europe/Asia/Australia Servers	25	NT4 Server	15	2003 Server
Europe/Asia/Australia P.C.s	120	NT4 Wrkstn, 9x	180	XP Pro
Total Global Computers	780		1250	

Figure 1 – Windows O.S. Dispersal snapshot for Camelot in 2001 and 2004

© SANS Institute 2005 Author retains full rights.

-1-

In the Beginning

"Computer viruses represent a significant and evolving threat to personal computers and department servers. Use, and regular update, of anti-virus software is a critical element of security protection"[2]

Camelot Corporation began its journey in what was typical for businesses running virus defense circa 2001. Camelot had in place what it considered to be the best available systematic options for defense at the time for its available resources. It had implemented McAfee VirusScan to its client computers and NetShield to its servers. Camelot had not even begun to look at policies or even to see a need to. At the time, hacking was a more salable threat and Camelot's efforts focused on firewalls, server patching and putting out fires.

Security Posture

Systems:

- **End User:** Camelot ran McAfee VirusScan version 3.x to 4.x on most client workstations. Many lab computers were not running virus defense. While all computers were deployed by I.S. with virus defense installed; some users often turned off virus defense when working in order to enhance their P.C.s performance. Non Windows Operating Systems on P.C.s also were not running virus defense.
- **Servers:** Camelot ran McAfee NetShield 4.x on most servers. Antigen was the primary line of defense for Camelot's mail system (Exchange). The AS/400 did not run virus defense. Older servers, or servers experiencing issues, were also without virus defense.
- **Overall:** The installations were performed, and client properties configured, by Camelot's internal I.S. department. System updates (DAT/Engine) were scheduled to occur at least twice a week with downloads occurring from McAfee's web site (http or ftp). The Help Desk would manually update DATs as events required.

Processes and Procedures:

- **Non-existent Guidelines:** Camelot had no formal policies or procedures in place to assist in governing virus defense efforts, or security in general.

[2] Rector and Visitors of the University of Virginia

© SANS Institute 2005 Author retains full rights.

Problem Description

- **Deployment:** Installation, reinstallation, or upgrade of virus defense for the 780 Windows based clients would take a minimum of 50 8 hour work days (Minimum 390 labor hours total to complete) with a more accurate assessment being a team of 3 requiring a month to complete the installations, with almost 60% of their time devoted to the effort (450 man hours).
- **Deployment Issue Recovery:** Problems during installations, reinstallations, and upgrades would often require intensive troubleshooting or rebuild of the affected system. This was a result of VirusScan being an invasive program, affecting key systems like the registry and services. The time to fix these issues is on top of the deployment resource consumption noted above.
- **Unmanageable:** Due to the nature of client based and controlled virus defense, these installations, configurations, status and operation could not be easily verified or controlled. E.g. if a system's virus defense failed or was turned off, I.S. would typically be unaware until the system had a problem that caused I.S. to verify virus defense status on the computer. The following were largely unmanageable under Camelot's available resources:
    - DAT and Engine Updates (Unable to guarantee successful and timely deployment)
    - Reporting and Metrics (Unable to produce real time, or even timely, and accurate reports)
    - Current Status Verification
- **Largely ineffectual:** Although, previously, the corporation's needs had not been formally identified, the virus defense system did not meet the corporation's needs or expectations. At least 1 virus a year would breach Camelot's defenses and impact internal systems (more than10 corporate systems affected at one time by the same virus). This was a direct result of the problems noted above with the system. Not all clients were guaranteed to:
    - Be running virus defense (or have it installed)
    - Have their virus defense DATs and Engine current
    - Follow appropriate security practices (No appropriate use policies in place to guide end users)
- **Internal Expenses:**

	Update Computers	Clean a Virus Outbreak
Labor Hours to Accomplish	432	200
Dollar Value per Labor Hour	15	15
Total Labor Cost	$6,480.00	$3,000.00
Yearly Total Cost of Virus Defense Efforts	$9,480.00	

Figure 2 – Cost of virus defense efforts over 1 year in 2001

© SANS Institute 2005 Author retains full rights.

- **Licensing and Vendor Support Expenses:** The cost of Camelot's licensing and vendor support in 2001 was approximately $30,000, including McAfee VirusScan, NetShield, and Antigen.

Camelot's virus defense efforts, licensing and a best guess of a yearly $10,000 in fix/rebuild expenses as an expense of VirusScan issues, would result in a best estimate of $50,000+ yearly. As noted above, this expense was largely ineffectual at meeting the corporation's needs or expectations. The system also created a general feeling of frustration and apprehension throughout the I.S. department.

Current Risks

"Expensive locks or no, the home-owner remains vulnerable. Why? Because the human factor is truly security's weakest link"[3]

Camelot's virus defense efforts, and their security efforts in general, could be considered as entirely at risk. While standard for the time, the corporation was not prepared to move into the future and was unaware of how poor their readiness was.

Also, the vast majority of Camelot's efforts were reactive, and tools to change that were not in place or were not available. Available resources did not allow for emergency deployment of DATs under any but emergency situations – For example, an infection.

Finally, no effective end user education was being done, either formally or informally. This actually represents the greatest risk to Camelot, as all of its efforts can easily be circumvented by one malicious or careless employee.

Impact of Industry Security Standards on the Situation

Camelot followed industry standard practices, often best practices, at the time in addressing virus defense and security as a whole. While industry leaders, like SANS, were predicting a future of zero day exploits and the need for Defense In Depth, the cost to benefit was not their yet for Camelot. Camelot also found itself quickly realizing the importance and potential impact of a Defense-In-Depth strategy.

[3] Mitnick, p. 3

© SANS Institute 2005 Author retains full rights.

-2-

The Construction of a Fortress

Camelot experienced a couple of key issues related to security that prompted the corporation to evaluate its position and look toward the future. The impact of viruses and expense of their clean up was one issue. The second key issue was the inability of I.S. to clearly define whether Camelot was appropriately secure to the corporation's management.

Proposed Solution

Camelot's owner defined to I.S., and the company, that the corporation's number one priority would be security for at least that coming fiscal year. I.S. responded by opening a new position in the department dedicated to security (Security Analyst), and formed a support team around that position (the Security Team). The Security Team consisted of existing I.S. employees and I.S. management, with participation by corporate employees or management as needed.

"Assessment is the first step any organization should take to start managing information risks correctly"[4]

In line with the logic that knowledge is power, The Security Team worked to identify Camelot's current security posture. The team developed a "Security Matrix" (see appendix here and here) to guide I.S. in assessment, planning and implementation of Camelot's security efforts. Two versions of the matrix are included in the appendix to demonstrate Camelot's growth and provide insight into Camelot's security map. The first two worksheets demonstrate the first incarnations of the tool, the latter three shows the more refined versions used more recently.

The matrix became an instrumental tool that suited Security Team assessment and planning needs. It could be easily used to define Camelot's current position, define key areas that needed addressing and give a numeric sense of Camelot's current posture (e.g. 7 out of 10). The placement of specific matrix line items was relevant to Camelot's interpretations and needs, and some decisions were obviously subjective. It was not meant to reflect what the Security Industry might have done, although best practices were one of the Security Team's key guides, and two externally provided security audits have validated the matrix as an appropriately designed tool.

[4] McNab, Preface p. xiii

© SANS Institute 2005 Author retains full rights.

I.S. then worked with corporate management to determine expectations and define goals for the Security Matrix. The corporation provided data and systems value classification. They also validated what needed to be accomplished and the priority in which the Security Team would achieve those goals. The defined goal set by the corporation relevant to this paper is:

- Average less than one virus infection per year.
- An infection is defined as a virus that impacts more than 10 P.C. systems at one time, or one or more server/network systems (Systems that typically impact more than 10 P.C.s or critical data).

The key requirements from the corporation related to this paper dictated the following efforts:

1. Implement a centrally managed and monitored virus defense system
2. Implement an inline virus defense appliance to scan SMTP traffic initially, HTTP, FTP and POP3 traffic eventually
3. Implement appropriate use policies and institute guidelines and end user education
4. Place virus defense on every computer that is attached to the LAN/WAN, with minimum 95% compliance.
5. Ensure that 90% or more of the clients report 1 DAT or Engine version old or newer (Current minus 1 or newer)

"Like so many things in the world of security, we have to practice defense in depth"[5]

1. **Implement a centrally managed and monitored virus defense system**:
   a. The Security Team sought a system that would:
      i. Allow for timely, if not real time, reporting
      ii. Allow prompt reaction to emergencies, including pro-active deployment of DATs and engines in emergency situations
      iii. Central control of client virus defense policies, eliminating the ability of the average user being able to disable virus defense on their systems, and ensuring that they were all appropriately configured.
   b. The Security Analyst then did an analysis of industry available virus defense tools. Camelot was already a McAfee subscriber, but reviewed other competitor's products as well (such as Symantec's). At the time no other company than Network Associates Incorporated (also known as McAfee – hereafter NAI) offered any tools close to what Camelot was looking to implement. NAI had a virus defense management suite called ePolicy Orchestrator, (hereafter ePO), and this suite was found to meet the defined needs and goals of Camelot.

[5] Wyk

© SANS Institute 2005 Author retains full rights.

c. Camelot elected to move forward with ePO because it offered:
   i. Centralized management
   ii. Policy Control of clients (including servers)
   iii. Centralized deployments, upgrades and updating
   iv. Excellent reporting capabilities in near to real time
   v. Pro-active capabilities
   vi. Could be used with standard architecture Camelot already had in place (SQL)
   vii. Agent Control of Clients – added assurance of compliance and communication

2. **Implement an inline virus defense appliance to scan SMTP traffic initially, HTTP, FTP and POP3 traffic eventually**:
   a. Part of the concern for the I.S. was the load on the Exchange server as it scanned for viruses in mailboxes and on the server itself – On Access Scan from McAfee's VirusScan product and the Antigen mailbox scans. The Security Analyst was asked to research appliances that might reduce the load on the Exchange server.
   b. The Security Analyst found that the best option for Camelot was to purchase NAI's product called McAfee's Web Shield Appliance (e500) because it offered the following:
      i. SMTP Traffic Scanning
      ii. Tie in to ePO reporting and monitoring
      iii. HTTP, FTP and POP3 scanning – Camelot had no intention of initially implementing this, but was looking to possible future use.
      iv. The device was an appliance, therefore adding no extra load to any other server and adding one more layer to our Defense-In-Depth strategy.
   c. The Exchange Server would be upgraded and Antigen retained to continue a virus defense system that did not put all Camelot's eggs in one basket (McAfee/NAI).

3. **Implement appropriate use policies and institute guidelines and end user education**:

As stated previously, the human factor is the most vulnerable facet of any security effort. While Camelot was trying systematically to provide the best defense possible, it also recognized the need to address this critical avenue of attack.

   a. No security policies existed at the onset of the new security effort.
   b. The security team would work to author, gain approval for and implement key security policies. The approval process would be multi-tiered, first from primary affected I.S. staff and their direct management; Second from the IS Management team; and finally from the Corporate Leadership (Management) Team.
   c. The Legal and Human Resource Departments would also be referenced and worked with, as appropriate, to ensure that no conflicts occurred between I.S. policies and other Camelot policies or government laws.

© SANS Institute 2005 Author retains full rights.

   d. The policies, after approval, would be posted to appropriate internal web sites and communication done with the Corporate Leadership Team to begin the process of introducing them to the corporation.
   e. I.S. will implement appropriate end user education, including instructing the Help Desk to:
      i. Properly respond to end users who have security questions
      ii. Instruct them in appropriate behavior
      iii. Point them to our existing policies and guidelines.
   f. The Security Analyst will also create low level best practice guidelines and instructions for end user use.
4. **Place virus defense on every computer that can run it that is attached to the LAN/WAN, with minimum 95% compliance**:
   a. Previously many systems were without virus defense, or had old versions or non functioning installations. This was seen as a critical vulnerability.
   b. ePO would be used to systematically deploy and ensure that systems were both up to date and operational.
5. **Ensure that 90% or more of the clients report 1 DAT or Engine version old or newer (Current minus 1 or newer)**:
   a. Previously many systems were without virus defense, or had old versions or non functioning installations. This was seen as a critical vulnerability.
   b. ePO would be used to systematically deploy and ensure that systems were both up to date and operational.

Solution Implementation

One of the key advantages to the timing of the implementation of ePO for Camelot was the fact that the company was moving to Windows 2000 (Professional and Server) near to the same time. Windows 9x and NT had shown repeated problems with uninstalling and reinstalling virus defense products, often requiring intensive Help Desk intervention to complete – or worse, requiring rebuilding the client computer. These concurrent implementations and deployments would help ensure the most pain free and successful project possible, and help ensure a much more successful virus defense effort in the future.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Implement a centrally managed and monitored virus defense system (ePO)

1. **System Setup**
    a. The server resides on a Windows O.S. (2000 originally, 2003 more recently)
    b. Database resides on a SQL database on a separate server
    c. ePO requires a wide range of ports to be open for agent / server communication. For this reason:
        i. Server was placed in the core with limited communication to any externally exposed system (DMZ or External)
        ii. Any systems not on the WAN/LAN were deemed to be acceptable to be out of communication with the server for extended periods of time. This decision later impacts reporting and compliance affirmation for those systems.
    d. See the appendix for layout maps, the first demonstrating initial configuration and the second demonstrating refined configuration utilizing the enhanced tools available in later versions of ePO, such as remote repositories.
2. **System Design and Process/Policy Setup**
    a. Active Directory User and SQL accounts (service accounts) created with appropriate permissions to be able to write to the database and install/remove/upgrade applications on client computers (including servers)
    b. The server was built and Database created
        i. Originally Windows 2000 server, more recently 2003
        ii. SQL Database housed on a separate server
        iii. Service account has permissions to write to SQL database
    c. Configured policies for controlled applications
        i. ePolicy Orchestrator Agent
            1. Do not allow client modification of policies
            2. Enforce virus defense application's operation
            3. Enforce policies every 5 minutes
            4. Communicate with ePO server every 8 hours (Server can 'wake' up the agents if an emergency communication is needed)
        ii. VirusScan 4.x (see common parameters below)
        iii. NetShield 4.x (see common parameters below)
        iv. More recently VirusScan Enterprise (7.x and 8.x) (see common parameters below)

© SANS Institute 2005 Author retains full rights.

v. Common parameters for VirusScan across all P.C.s
    1. Scan all files, attachments, and compressed files
    2. Attempt to clean, if can't clean – delete
    3. Scan on read and write (access)
    4. DAT and Engine update scheduled every day at 8 A.M.
    5. Local Drive Scan configured to run every fourth Thursday of the month
    6. More recently, with additional spyware scan functions included with Version 8 of VirusScan Enterprise, scan is now configured to look for spyware (top 200 threats) and unwanted/joke programs

vi. Common parameters for VirusScan/NetShield across all Servers
    1. Scan all files, attachments, and compressed files
    2. Attempt to clean, if can't clean – delete
    3. Scan on read (access)
    4. DAT and Engine update scheduled every day at 12 A.M.

vii. Exceptions
    1. Certain servers and P.C. clients have exemptions to common parameters if required for essential business functions to operate. For example: Exclusion of certain directories or extensions from scanning.
    2. Certain P.C. lab clients are not running virus defense due to interference with business critical functions

d. Target computer list imported from Active Directory computer client list
    i. Generated an unverified list of potential ePO clients
    ii. Verification of existence of the computers would be a later step for those the agent couldn't deploy to

e. Initial ePO Agent deployment done through systematic capabilities of ePO
    i. To attempt deployment of the agent to all 800 computers required merely right clicking and doing a Send Agent function – This is an immense improvement over past deployment efforts which involved desk side visits.
    ii. Agent deployments take an average of 15 minutes to deploy on active computers
    iii. Continued to attempt deployment over the next month to ensure that all computers were given every chance to become available and receive the agent

f. Concurrent to Agent deployment, whenever an agent is successfully deployed it installs the designated version of virus defense and applies appropriate policies as configured in ePO

© SANS Institute 2005 Author retains full rights.

g. Designed ePO Server's directory structure to ensure appropriate policies could be configured.
    i. ePO uses an MMC interface (Microsoft Management Console)
    ii. Client directory structure is similar to Active Directory Users and Computers
    iii. Organized client structure based on function and geographic location:
        1. Foreign Branch Offices had their own groups
        2. U.S. Corporate Headquarters had its own group (all 4 buildings in one group since they reside in one city)
        3. U.S. Branch Office in its own group (one physical location)
        4. Offsite Sales Personnel in their own group (multiple users spread out across the U.S.)
        5. Servers in their own group in an appropriate geographic subgroup as applicable
            a. Development
            b. Production
        6. Lab Computers in their own group in an appropriate geographic subgroup as applicable
        7. Rarely Connected Computers in their own group in an appropriate geographic subgroup as applicable
            a. Checkout Computers
            b. Meeting Room Projector Computers
            c. Department / Group / Multiple User computers
        8. I.S. Computers in their own group
    iv. This configuration optimized Camelot's ability to:
        1. Deploy updates, new versions, upgrades and other client deployments at a time appropriate to widely varied business hours
        2. To configure local repositories that would stop the need for clients in Europe/Asia downloading multi-megabyte downloads across the ocean from the U.S. Instead they download all their updates from their own local branch. This reduced deployment times from 4+ hours with high failure rate to less than a half hour with almost 100% success.
        3. To allow for test groups, testing of policy changes and new applications/updates
        4. To allow reports to more easily isolate incorrect information (rarely connected computers are more easily identified, eliminating them from skewing report results)
            a. Track down problem areas more easily
            b. Identify needed data faster
            c. Provide more valuable data

© SANS Institute 2005 Author retains full rights.

5. To allow policies to be applied appropriately
    a. Servers separate from P.C.s
    b. Development Separate from Production allowing for testing on Server Platforms
    c. Foreign Branch Separate from U.S. to allow for local repositories and varied time zone implications
    d. Exclusions can be applied to like computers (Lab computers or servers for instance)

h. Performed, and continue to perform, client verification
    i. When a computer can't be deployed to, or the agent has been out of communication for an extended period of time, I.S. attempts to locate the computer and determine what the issue is
        1. Does it exist
        2. If not, remove it from ePO and Active Directory
        3. if it does, fix it
    ii. This process helps keep both ePO and Active Directory reasonably current. Unfortunately limited resources often impact the ability of I.S. to stay on top of this.

i. Perform ongoing analysis, reporting, maintenance of the system
    i. The Security Analyst is solely responsible for ensuring Camelot's virus defense efforts are appropriately up to date
    ii. Daily verification of status occurs to ensure new clients are moved to appropriate groups

j. Added systematic deployment of agent to all Domain computers through:
    i. Logon Script verification of the agent being installed and running
    ii. Installation of the agent on all Images used for P.C. deployment (Camelot uses Remote Installation Services for P.C. deployment)

k. Instituted I.S. policies that dictate process and procedure for deploying new clients and recovery of old clients that help to ensure all databases (ePO and Active Directory) are kept up to date and virus defense is deployed before the computer leaves I.S. control

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Implement an inline virus defense appliance to scan SMTP traffic initially, HTTP, FTP and POP3 traffic eventually

1. **System Setup**
    a. e500 WebShield server appliance runs on a Linux O.S.
    b. Requires that traffic to be scanned be forwarded to it, and then traffic is rerouted after scanning
        i. SMTP traffic goes first to the e500 (e1000 more recently) where it is scanned and then rerouted back to the Exchange server for delivery
        ii. If HTTP, FTP or Other traffic is to be scanned would require all clients use the WebShield appliance as a proxy – Camelot is in process of debate over cost to benefit of this move
2. **System Design and Process/Policy Setup**
    a. The system is configured to scan all SMTP traffic
        i. Branch office mail goes first through U.S. through the WebShield appliance
        ii. Scans all attachments, files and email
        iii. Scans inside compressed files
    b. Deletes attachments having specified extensions
        i. .exe
        ii. .scr
        iii. .sys
        iv. Etcetera
    c. Updates DAT files on a daily basis

Implement appropriate use policies and institute guidelines and end user education

1. Have instituted the following policies/Guidelines
    a. How do I protect my system from computer viruses
    b. What do I do if I receive word of a virus or warning by e-mail?
    c. What can you do to help prevent security incidents?
    d. Appropriate Use (4 pages)
2. The Appropriate Use policy was approved by the Corporate Leadership Team, Human Resources, and the Legal Department
3. The Appropriate Use policy has been communicated to key management and a company wide communication effort is being planned
    a. To be successful end users must understand and support the policy
    b. Need to have a base level of understanding (education) for the company to allow this to be fully effective (see education bullet below)
4. More guidelines, best practices and educational documents are in the works
5. The Security Team is working with Corporate Management to institute a security education program and material for this program is currently being generated

© SANS Institute 2005 Author retains full rights.

Place virus defense on every computer that can run it that is attached to the LAN/WAN, with minimum 95% compliance.

1. The Security Analyst and the Help Desk work together to ensure that every computer deployed, upgraded or touched by them are running virus defense and that it is current
2. The Security Analyst works with ePO to ensure systematically that all computers are running virus defense and that it is current
    a. Systems that are not current are tracked down and troubleshot or determined not to exist anymore
    b. Systems that can't be found are removed from Active Directory to ensure minimal danger to the domain
3. Added systematic deployment of agent to all Domain computers through:
    a. Logon Script verification of the agent being installed and running
    b. Installation of the agent on all Images used for P.C. deployment (Camelot uses Remote Installation Services for P.C. deployment)
4. Instituted I.S. policies that dictate process and procedure for deploying new clients and recovery of old clients that help to ensure all databases (ePO and Active Directory) are kept up to date and virus defense is deployed before the computer leaves I.S. control

Ensure that 90% or more of the clients report 1 DAT or Engine version old or newer (Current minus 1 or newer)

1. The Security Analyst and the Help Desk work together to ensure that every computer deployed, upgraded or touched by them are running virus defense and that it is current
2. The Security Analyst works with ePO to ensure systematically that all computers are running virus defense and that it is current
    a. Systems that are not current are tracked down and troubleshot or determined not to exist anymore
    b. Systems that can't be found are removed from Active Directory to ensure minimal danger to the domain
3. Added systematic deployment of agent to all Domain computers through:
    a. Logon Script verification of the agent being installed and running
    b. Installation of the agent on all Images used for P.C. deployment (Camelot uses Remote Installation Services for P.C. deployment)
4. Instituted I.S. policies that dictate process and procedure for deploying new clients and recovery of old clients that help to ensure all databases (ePO and Active Directory) are kept up to date and virus defense is deployed before the computer leaves I.S. control

© SANS Institute 2005 Author retains full rights.

-3-

After

The current deployment of ePolicy Orchestrator, VirusScan, the WebShield Appliance, Antigen, Policies and Procedures, and Guidelines work together to provide a significantly enhanced virus defense stance and improved security in general.

As demonstrated earlier, the total yearly cost of virus defense in 2001 was approximately $50,000. The current cost is significantly lower:

	Update Computers	Clean a Virus Outbreak
Labor Hours to Accomplish	24	0
Dollar Value per Labor Hour	30	30
Total Labor Cost	$720.00	$0.00
	Manage the Centralized System	
Labor Hours to Accomplish (yearly)	300	
Dollar Value per Labor Hour	$30.00	
Total Labor Cost	$9,000.00	
Yearly Total Cost of Virus Defense Efforts	$9,720.00	
Licensing and Vendor Support Costs	$31,000.00	
Yearly Total Cost of Virus Defense including Licensing and Support	$40,720.00	
NOTE:		
Number of Computers In 2001	780	
Number of Computers in 2004	1250	

Figure 3 – Cost of virus defense efforts over 1 year in 2004

© SANS Institute 2005 Author retains full rights.

In addition to being a lower overall cost, (or break even if you don't count indirect costs noted in the 2001 figures) the results are much improved:

1. In the years since implementation of ePO, Camelot has been Virus Incident free (as defined previously) – not one breach in approximately 3 years.
2. Not only has the cost to deploy new versions and updates gone significantly down, it has increased success of deployments and allowed verification of that success.
3. Where, prior to these efforts there was no reporting available, a plethora of invaluable reports exist in near real time status:
    a. DAT compliance
    b. Engine Compliance
    c. Infection Reports
    d. Infection Patterns
    e. Top 10 lists (most attacked computer, most attacked user, most prevalent virus…)
    f. Etcetera
4. Where previously our virus defense status was never truly known, the Security Analyst can now assure management of our status on a moments notice and show a proven track record of success.
5. The policies and procedures we have implemented have moved us from a best estimate of 50% compliance to VirusScan deployment, DAT and Engine compliance to a minimum 90% compliance with the vast majority of the remaining 10% being unable to comply due to special circumstances
6. Our Defense-In-Depth strategy has resulted in an average of 90% of all viruses being cleaned prior to even reaching the end user (typically the mailbox of an end user). In other words, P.C. based VirusScan only catches a maximum of 10% of the viruses caught by our company – and that figure is high.

Additionally, the improvements made over the years to both NAI's and Microsoft's products have resulted in a more stable environment all around. Fewer issues occur due to VirusScan conflicting with operation of a computer's O.S. In 2001 the incidents occurred almost weekly. In 2004 we have not seen one incident that could be clearly pointed to an issue with VirusScan / Operating System conflicts.

Solution Testing and Validation

The existing system continues under a daily barrage of virus attacks. Its validation occurs daily as its success continues to protect Camelot from viruses and reduce cost of management and implementation.

© SANS Institute 2005 Author retains full rights.

Risk Assessment

Some key risk areas continue to exist:

1. Camelot still needs to address a couple primary areas of virus defense program implementation: The non-Windows operating systems at Camelot are largely unprotected. Camelot is currently working on this issue.
2. End user education and instructional documents and guidelines still have not been fully implemented or communicated. As noted earlier, this is a critical step towards a much enhanced virus defense (and security defense in general) posture. Camelot is working on this initiative currently.
3. Resources are limited and some work that should be done in a timely fashion is not always accomplished. Camelot could do a better job of ensuring compliance to systematic policies for instance.
4. Virus defense, for all it has improved, continues to be primarily a reactive technology. Because of this, zero day exploits or exploits we don't even know about continue to be a threat not easily countered.
5. Spyware is quickly becoming a larger threat than viruses. Camelot's top concern at this point is this relatively new avenue of attack. Due to its insidious nature it can cause more damage without actually exposing itself than typical viruses. While VirusScan Enterprise 8.x has implemented Spyware scanning, it, and no other product, has proven capable of handling every known Spyware threat.

Conclusion

Camelot can count its efforts a resounding success, but should be wary of the future and continue to be vigilant. As is often pointed out by security experts, security is a game of leap frog, with white hats improving defenses and black hats finding new avenues of attack. If Camelot remains stagnant, then its security efforts will be for naught.

Additionally, Camelot should be proud of the way it was able to gain cooperative effort throughout the corporation, involving multiple departments, and even the whole company, in some of its efforts. Every employee plays an important role in security, and Camelot has a great user base to work with. The users are intelligent and concerned and show a desire to do what is needed and what is right.

© SANS Institute 2005 Author retains full rights.

References

1. SANS. "Windows XP: Surviving the First Day", University of California, Berkeley Web Site, 23 Nov, 2003, URL: http://ist-socrates.berkeley.edu:2002/bestpractices.html 26 Nov, 2004

2. Rector and Visitors of the University of Virginia. "Security Best Practices", University of Virginia Information Technology and Communication Web Site, 30 Jun, 2003, URL: http://www.itc.virginia.edu/security/vulnerabilities.html 26 Nov, 2004

3. Mitnick, Kevin D. The Art of Deception, Indianapolis, Wiley Publishing 2002, p. 3

4. Mcnab, Chris. Network Security Assessment, Sebastapol, O'Reilly Publishing 2004, Preface p. xiii

5. Wyk, Kenneth van. "Blaming Users for Virus Chaos?", eSecurityPlanet.com Web Site, 6 Jul, 2004, URL: http://www.esecurityplanet.com/views/article.php/3377201 26 Nov, 2004

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Appendix

Security Matrix – Old

Overall Security Assessment

See Charts and Graphs

Figure 4

Assessment by Technology Risk Area

See Charts and Graphs

Figure 5 Figure 6 Figure 7 Figure 8

Security Matrix –Recent

The New Security Matrix Key

See Charts and Graphs

Figure 9

Overall Security Assessment

See Charts and Graphs

Figure 10

Assessment by Technology Risk Area

See Charts and Graphs

Figure 11 Figure 12

Assessment by Attack Vector

See Charts and Graphs

Figure 13

ePolicy Orchestrator System Layout

Original

See Charts and Graphs

Figure 14

Recent

See Charts and Graphs

Figure 15

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

How do I protect my system from computer viruses:

NOTE: Please do not send company notices of viruses. If you hear of a virus, please contact the Help Desk at x001 so they can verify the threat and then notify all users if appropriate.

Recommendations:

1. Ensure your virus DAT files up to date and run Virus Scan on a regular basis. Virus Scan has been configured to automatically download and install the updated DAT file on a regular basis, but you are free to check on your system's status and update it if it is out of date. VirusScan is also configured to automatically do a scan on your system the fourth Thursday of every month, you are free to run the scan more often.

2. Use caution when opening any attachment files that you are not expecting and/or from people you do not know. If in doubt about the attachment content, DO NOT open it. Save it first, run Virus Scan on the file and if it's safe then open it.

3. If you note that VirusScan is out of date or is not running correctly, contact the Help Desk immediately.

If you have any questions about VirusScan, please contact the Help Desk at x001 for assistance.

What do I do if I receive word of a virus or warning by e-mail?

Please be aware that **not** all virus notices or warnings received from external sources are accurate. There are many that are actually hoaxes. Below are links to sites that provide information regarding actual and hoax viruses:

http://vil.mcafee.com/hoax.asp
http://www.f-secure.com/virus-info/hoax/

NOTE: Please do not send company notices of viruses. If you hear of a virus, please contact the Help Desk at x001 so they can verity the threat and then notify all users if appropriate.

© SANS Institute 2005 Author retains full rights.

What can you do to help prevent security incidents?

- Keep your password secure:
  - Don't write your password down
  - Don't use family members' names or birthdates, anniversary dates or pets' names
- Do not open any attachment in email or instant messaging without being sure of the person who sent it to you, and what it is. Always copy that attachment to a network (G:\ or H:\) or local (C:\) drive before opening.
- Don't open any attachment in email that is a movie, screensaver, game or program (also called "executable") unless it is directly related to Camelot business.
- **NEVER** disable your VirusScan when you are browsing the Internet or using Outlook or reading email through any source. **VirusScan should never be disabled without the approval of Information Systems.**
- Do not install any program on your local computer or the network without getting approval from Information Systems. The Hardware/Software Request form can be found at (internal link). When evaluating these requests, Camelot seeks to ensure not only user need and financial appropriateness, but also the security and integrity of our computing environment.
- Don't go to any website you are not sure is legitimate. Avoid websites or web pages having anything to do with the following:
  - Online gaming
  - Online gambling
  - Pornography
  - Hacker sites
  - Any sites that are questionable in content or you aren't sure of the content
- When visiting websites do not download or install anything that you are not sure is a legitimate file.
- Always ensure your computer is locked when walking away from it by pressing Ctrl-Alt-Delete>Lock Computer.
- Watch for actions that contribute to security incidents:
  - Is someone logging into the network as someone else?
  - Is someone able to access something they probably shouldn't be able to?
  - Is someone copying or e-mailing Camelot's proprietary data outside the company?

If you have any questions, please contact the Help Desk at x001 for assistance.

© SANS Institute 2005 Author retains full rights.

Camelot Computing Security & Acceptable Use Policy

1.0 Purpose

This policy will address acceptable use of Camelot's computing infrastructure to help ensure the integrity of the security of Camelot's assets.

2.0 Scope

All Camelot employees, work associates, consultants or anyone utilizing Camelot's computing assets are included in the scope of this policy.

3.0 Policy

1. Security - General Computing
2. Security - Password Requirements
3. Security - Computer Virus Protection
4. Security - Wireless Access
5. Security - Portable Devices
6. Acceptable Use of Computing Resources

1. Security - General Computing
    a. Only hardware and software that have been approved for Camelot use may be installed on Camelot Personal Computers. The IS Hardware/Software Request Form (link to internal web page) on the Court of Camelot (Internal Web Page) is the primary method to request approval for new services. Contact the Camelot IS Help Desk with any questions. Any software considered to be a likely security risk will not be permitted on a Camelot Personal Computer.
    b. New devices may not be physically attached to Camelot's corporate network without appropriate approval from the Camelot IS Help Desk. This includes, but is not limited to, desktops, laptops, wireless devices, hubs, routers, switches, PDAs, and printers. Improperly configured or unprotected additions to the network can cause serious company-wide problems and can provide easy security targets.
    c. Corporate computing security tools (e.g. virus defense) may not be turned off or circumvented without appropriate approval from Camelot's IS Help Desk. Employees are expected to contact the Camelot IS Help Desk if they note any security tools that are not functioning correctly, not installed or are out of date. A single security hole can put the entire network at risk.
    d. Employees should not remotely connect to Camelot's Network without appropriate security in place. For example, if connected to the Camelot Network using a home PC, that home PC should be running virus defense that is up to date and operational and the system should be fully patched. The home network should also have an appropriate firewall in place.
    e. Employees should immediately report any suspected computing security incidents to the Camelot IS Help Desk.
    f. Camelot employees are each personally responsible for following the guidelines outlined in this document. In addition, employees are expected to exercise good judgment regarding the use of Camelot's Computing

© SANS Institute 2005 Author retains full rights.

Resources. Many security events can be avoided by using common sense.

g. Guidelines for safe computing can be found at the IS Security Website (link to internal web page) or by contacting the Help Desk.
h. System tools to troubleshoot or resolve issues with computers should not be used without first contacting the Help Desk. Many of these tools have the potential to cause as well as fix problems. In using these tools you may do more harm than good. Before taking any action to resolve a problem with your computer, other than closing and restarting any affected applications or rebooting your computer, please contact the Help Desk. Examples of these types of applications include System Restore, Backup; Disk Clean Up, File and Settings Transfer Wizard, etc.

2. Security - Password Requirements
    a. The following are the requirements for all Camelot computing passwords. These requirements are systematically enforced on our Domain.
        i. All passwords will be at least 7 characters long.
        ii. All passwords will contain a character from at least 3 of the following categories:
            1. A number (0-9)
            2. A lower case letter (a-z)
            3. An upper case letter (A-Z)
            4. A non alpha-numeric symbol (!@#$%^&*(-)+=_)
        iii. No password may contain the user's username, nor may it contain their first name of last name.
        iv. None of the previous 5 passwords may be reused.
    b. All user accounts will require password changes at least once every 90 days. This policy is also systematically enforced.
    c. Passwords should not be written down and then left in a non-secure location.
    d. Account information, including username and/or password, should not be given out to non-Camelot employees.
    e. Passwords should not be shared with anyone at Camelot, including IS, without verification of appropriate business need and verification of identity. Bold hackers have been known to walk into companies and obtain security clearance from overly helpful employees. If account information has been shared with an internal employee to meet a valid business need, the password should be changed as soon as possible after the work is completed.
    f. If an employee suspects their account or password information has been compromised, they should change their password immediately and contact the Camelot IS Help Desk.
3. Security - Computer Virus Protection
    a. Camelot has established systematic centrally managed virus defense configurations. All Camelot computers will run the Camelot standard for virus defense software. These configurations shall not be circumvented

© SANS Institute 2005 Author retains full rights.

locally or changed without appropriate approval from the Camelot IS Help Desk.

b. Employees are responsible to cooperate with all Camelot efforts to keep their systems up to date, including assisting in updating systems if central management is unable to systematically apply updates.
c. Employees are to report to the Help Desk any systems that are not running appropriate versions of virus defense or where virus defense if not operating correctly so that the problem can be corrected quickly.
d. Computer users who are offsite and are not typically connected to the LAN or WAN (for example the Field Sales) are responsible to ensure their anti-virus signature files (DATs) are updated at least weekly. Daily auto-patching of virus signature files (DATs) is recommended. Instructions are posted on the IS website (Link to internal web site).

4. Security - Wireless Access
    a. All corporate network wireless devices must be approved, configured and installed by IS to ensure appropriate security configuration. Improperly configured wireless communication is highly susceptible to security problems.
    b. Once enabled for wireless connection, users are responsible to ensure their wireless device's configuration is not altered.
5. Security - Portable Devices (laptops, PDAs and similar devices)
    a. Employees are to immediately report any lost or stolen portable device so that appropriate measures can be taken to reduce risk to the network systems.
    b. When traveling or away from the office, employees need to be aware of the threat of computer theft and take actions to appropriately secure Camelot's portable computing devices.
    c. Employees are encouraged to periodically back up important data to a location not on the portable device to prevent loss of that data in the event of hardware failure or theft/damage.
    d. When traveling, sensitive data should not be kept on portable devices unless absolutely necessary. If necessary, then the data should be properly encrypted. Contact the Help Desk for further information regarding encryption. Encryption software can be requested through the IS Hardware/Software Request Form (link to internal web site).
6. Acceptable Use of Computing Resources
    a. Camelot's computing resources may not be used for Streaming Audio or Video access unless directly related to Camelot's business. These services use significant network bandwidth and impact the performance of legitimate Camelot business use of the network.
    b. Camelot's central disk space may not be used for downloading and storing personal images, music, video or other personal data files.
    c. Camelot's computing resources may not be used for Peer to Peer (P2P) file sharing services (e.g. Kazaa or Morpheus MP3 sharing). These services can be a source of viruses, use significant bandwidth and often have legal implications.

© SANS Institute 2005 Author retains full rights.

d. Personal email accounts may not be downloaded directly to Camelot's email client software (Outlook for example). Personal email services include AOL, Yahoo, MSN, or similar providers. Directly loading email from these services circumvents the Camelot security defenses and can introduce viruses and Trojan backdoor software onto the corporate network. Checking external email via that email provider's web interface is a secure method of viewing personal email.
e. Camelot's computing resources are intended for business use. Excessive personal use is not permitted as it impacts employee productivity and Camelot costs. This includes but is not limited to: personal email, personal telephone costs and personal instant messaging.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Charts and Graphs:

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**