Internet Usage for Commodity Broker Access

A Case Study

Implemented during the months of Mar – May 2001

Wayne T Work, Sr.
Certified Information Systems Security Professional (CISSP)
Sr. Information Systems Security Consultant
May 26th 2003

The Premise

A very profitable Commodities broker located in the Southwest portion of Connecticut is faced with the rising costs of long distance phone access and lack Internet facing access. The secondary issue is access for mobile users as they have presently and in the near future, numerous external users, located in several countries throughout the world.

This corporation does approximately 1 Billion dollars in "real-time" transactions and trades each day. The need to increase accessibility and add a layered functional security model is essential to the profitability, liability and sustainability of the corporation.

The Assessment of Present Infrastructure

A detailed analysis of their business model and needs assessment were performed. These assessments took into consideration the "Normal" business practices and the "Normal" day to day needs of the corporation and its remote users (Commodity Brokers located in numerous countries). A detailed analysis of present the infrastructure systems, the computing environment and application functions and access which are used for normal business trading were taken in to close scrutiny. The following are some of the areas of consideration during the assessment.

- The business structure of application access within the current environment
- The need for "Real-Time" transaction access to current applications
- The current Computer Servers in production
- The Current Internet access that is presently being used for administrative processes
- The Firewall and Internet controls being used in the current environment
- Time of access to applications due to world wide usage
- The Bandwidth needed for concurrent access to all applicable applications

The Findings

After performing an extensive analysis of the corporation's environment, Internet facing presents and business practices, the following was noted:

- The business practices of this corporation requires a very diverse ability to access all trading applications worldwide with a substantial emphasis on security of the data
- The corporation does not have any valid domain names pointing to the external Internet IPs used by the corporations Internet Access. This does not allows a "Cracker" to gain any positive knowledge of the external Internet IPs for this corporation
- The use of Enterprise level Firewalls and Intrusion Detection Systems which are in place in the current infrastructure provide a robust level of initial access to and from the Internet

- The current Computer Servers used to host the trading applications are not sufficiently secured for external access without substantial "Lock Down"
- There is currently no authentication mechanisms in place to adequately insure proper access to trading applications
- The bandwidth is sufficient for normal operations and access to the critical applications

The Remediation

The current corporation infrastructure will support, with some required modifications, the introduction of the Internet as a viable, secure and cost effect method for allowing access to the current application used for commodity trading by external "Trusted" users. The following are the remediation efforts that should be implemented prior to any access of internal applications from the Internet.

- The Computer Servers that are used to host the applications were "Locked Down" (This is a process of removing services and unneeded applications/OS programs which may reside on a computer which increase risk and reduce the security posture of the Server)
- Specific rules for the firewall and IDS system were implemented. These rules were specific to only allow specific access to specific applications on specific Servers.
- Routers and Switches were configured to route specific traffic and access to specific Servers
- Access to each applications was limited via a Citrix Metaframe implementation which was closed to allow only "Published Application" access to the Internet
- An extensive authentication process was implemented. This processed use RSA's Secure ID, ACE Servers, a very customized and controlled Nfuse Web Portal and a series of servers which were placed in between the Citrix Metaframe Servers and Server Farm and the Internet Gateway Appliances Firewalls, Routers and Switches.
- Detailed Policies and Procedures document was developed and implemented which clearly explained all aspects of the process and procedures which were used to provide the maximum Confidentiality, Integrity, Authorization, and Accountability of al accessed to all applications that are dedicated to this process.
- All processes and procedures were verified for compliance of all Securities and Exchange Commission requirements and regulations.

The Conclusion

The culmination of the above efforts and processes added a great deal of security, reliability and access for all remote Commodity Traders throughout the world. The cost of Long Distance phone calls, the reduction of Dedicated Internet access and the security of data transfer saved this corporation thousands of dollars per month and reduced the

liability of performing eBusiness to a risk level which was totally acceptable to both the corporation and the SEC.