12 Elmwood Road | Albany, New York 12204
888.400.7938 | www.tagsolutions.com

SUCCESS STORY
ENTERPRISE SECURITY
AND COMPLIANCE

Rapid response and security expertise keep national not-for-profit running

The Challenge:

TAG Solutions was contacted and asked to provide security assistance to a national enterprise client with more than 30 locations. An initial telephone interview indicated that the organization was experiencing an assumed virus outbreak that had caused debilitating network outages and crippled business operations. The client technology environment provided numerous attack vectors for unwanted viral activity, and their lack of security management tools limited their ability to distribute remediation solutions to the affected desktops. How would the dispatched team of TAG Solutions technicians quickly and efficiently contain the threat, restore network functionality, deliver incident response guidance, and provide remediation options to the client technical team?

The Solution:

The TAG Solutions response methodology aimed to determine the incident scope and risks, contain the spread and impact of the threat, restore network services and develop procedures that would eradicate future threat. Utilizing sniffer and traffic analyzer tools, TAG Solutions was able to determine what parts of the client network were affected and that the presence of IRC traffic was the major cause of the outages. Proper configuration of the firewalls at all 31 remote locations and implementation of a Microsoft provided patch management solution contained the virus. Anti-virus software upgrades were made to network servers to prevent retrovirus activity. Desktop firewalls were enforced and configured to stop the spread of network-based viruses to other devices. Finally, TAG Solutions security analysts developed a custom script to assist in removing the immediate threats and upgrade the level of future protection.

The Return:

Within 24 hours of first response, the threat had been contained and most of the 31 remote network locations were able to conduct work at degraded speeds. By day two, all solutions were in effect and network operations had been restored to pre-incident speeds and capabilities. A nationwide deployment of the custom threat eradication script was successful and ongoing testing of the client network has shown no signs of subsequent threat intrusion.