Security Assessment

Situation

ZAG Technical Services, Inc. was called in by a Bay Area based company to perform a security audit of their network. The focus of this review was to audit security from the perspective of the Internet.

Solution

ZAG utilized a host of scanning tools to perform this audit. During this audit, many security issues were identified. These security issues included the obvious, such as having unnecessary ports allowed in, to inadequate patch levels on servers that were accessible from the Internet.

The results were documented and delivered to the customer for their review. Upon reviewing the results with ZAG, the customer requested that ZAG implement changes to their network to ensure their security.

ZAG completely reconfigured the firewall to ensure that only what truly needed to get into the network was allowed in. ZAG also changed the firewall to only allow those ports out that the company approved of. This greatly assisted in securing the environment and will, in worse case, help to mitigate the problems that may arise from virus outbreaks and other dire incidents.

ZAG next patched the customer's servers to ensure that they were no longer susceptible to exploits. Other steps such as changing the Administrator password were also taken.

Next, ZAG was asked to perform a review of the local security on the network. ZAG found several issues in this review and documented and reviewed them with the customer.

As a result of this review, ZAG implemented Trend ScanMail for Exchange on the customer's Exchange server. ZAG also deployed Norton Corporate Edition in a centrally managed configuration to ensure that desktops were protected. It was felt that doing two separate virus solutions would further protect the customer by having two different points from which current virus definitions could be pulled.

Next, ZAG deployed Microsoft's Software Update Service (SUS) and forced management of the local desktops. This ensured that the local desktops were protected from known exploits.

Finally, ZAG implemented security at the password level to ensure that the company resources were protected.

Benefits

These changes, as well as some not referenced in this Study, made it so that the customer's network was secure. As the owner of the company stated, "Having ZAG come in and secure our network was a relief. I couldn't believe how utterly unprotected we were."