SecureWave
Safeguarding Tomorrow

by SecureWave
Sanctuary
Application and Device Control

First National Bank of Bosque County

Full service consumer bank replaces anti-virus and anti-spyware products with Sanctuary Application Control

Background

The First National Bank of Bosque County (US$86 million in assets) is a full-service consumer bank headquartered in Valley Mills, Texas, a community about 20 miles west of Waco. The bank has four branches throughout the area and offers a complete selection of deposit and lending services, as well as mortgage loans and merchant credit card acceptance services. The bank's IT environment consists of 42 computers and seven servers across its four locations.

Challenge

In March of 2006, Brent Rickels, the bank's vice president in charge of technology - and the lone member of the IT staff - decided to re-evaluate the bank's security infrastructure. The bank's Symantec desktop anti-viruses licenses were set to expire and Rickels questioned the value of renewing them.

"Auditors love to see that we are staying ahead of potential challenges, so everything we do around here is proactive by nature. I wanted our approach to security to be the same way," said Rickels. "We were having our fair share of spyware problems despite deploying anti-spyware software. It was obvious that because anti-virus and anti-spyware solutions are reactive by definition, they did not offer the complete malware protection we were after."

Also, because Valley Mills is a developing area, the bank only recently acquired the infrastructure needed to establish a dedicated internet connection. Rickels analyzed the risks associated with this type of dedicated connection and anticipated that there may be problems.

"Even if you have a clear written policy, people will still log on to Web sites that they should not be going to," said Rickels. "Without a comprehensive enforcement solution, you still have to depend on users to manage their own computers and inevitably, you will have some employees either purposely or unintentionally create a problem."

Solution and Benefits

After evaluating several technologies, Rickels elected to purchase Sanctuary Application Control from SecureWave. Sanctuary enables users to whitelist allowed applications, denying all other executables by default. This includes all forms of malware and all unauthorized and unwanted software. "We looked at a variety of solutions from many different vendors, but most were reactionary and others only isolated and quarantined malicious executables. Sanctuary actually prevents them from running, and it is far easier to manage," said Rickels.

With assistance from SecureWave engineers and Sanctuary's automated whitelisting feature, Rickels scanned the bank's computers and built the application whitelist in a single day. Installing the client piece took about three minutes per machine, and Rickels was able to do this from his central workstation.

To demonstrate to bank employees how Sanctuary works, Rickels blocked Windows games from running. People who tried to run Solitaire or Minesweeper received a pop-up message explaining that those applications were not allowed. "This showed users how non-intrusive Sanctuary is. Fortunately, whitelisting is a very easy concept for all employees to understand, regardless of their technical know-how," said Rickels.

Two other applications that Rickels elected to keep off the whitelist are all peer-to-peer and instant messaging (IM) programs. "The disadvantages to using IM far outweigh the advantages," said Rickels. "There is no way of knowing what might be leaving the bank via IM, traffic cannot be monitored effectively and now, IM is even a way for viruses to get onto machines. The best thing to do is just block these programs."

Because Sanctuary effectively prevents all viruses, spyware and other malware from executing, Rickels elected not to renew his desktop anti-virus and anti-spyware licenses. "The differences between solutions that use a blacklist versus those that use a whitelist are tremendous," said Rickels. "The anti-virus and other blacklisting solutions are controlled by a third party but we are able to completely control the whitelist of allowed executables. Also, a blacklist can never be complete because of the myriad of new viruses being introduced

every day. A complete whitelist is easy to construct, and it only changes when we need it to."

Rickels also plans to upgrade to Sanctuary 4.0, the industry's only solution that enables organizations to enforce policies for both applications and devices.

"Device security has not been a problem for us, but as I said, we like to be proactive and address potential issues before it is too late," said Rickels. "Some people are starting to use memory sticks to carry their work with them. We need to make sure that nothing is leaving the bank that we do not know about. Portable storage media is also becoming a mechanism for transferring viruses and other malware. With Sanctuary 4.0, we will be able to enforce our policies regarding proper application and device use on bank computers."

Conclusion

Since deploying Sanctuary, the First National Bank of Bosque County has not experienced a single spyware incident and no other malware has infected any of the bank's machines. Prior to Sanctuary, Rickels spent hours every week checking each machine for viruses and making sure the anti-virus was set up correctly and properly updated. Now, the only time Rickels spends updating the whitelist is on Patch Tuesday.

"I spend about an hour per month updating Sanctuary," said Rickels. "I am able to deploy the patches at my own pace because I know that Sanctuary will prevent any of the vulnerabilities from being exploited. The administrative overhead required to manage Sanctuary is very minimal."

"Sanctuary solves all your problems," said Rickels. "It is cheaper than anti-virus so it has paid for itself already. Dropping one vendor in favor of a less expensive, more effective one is pretty much a no-brainer."

SecureWave
Safeguarding Tomorrow

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23 - ZA Bourmicht
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

www.securewave.com
info@securewave.com