BLACKTHORN
INFORMATION SECURITY
P.O. Box 64784 • Burlington, VT 05406 • (802) 373-0322 • www.BlackthornInfoSec.com

Case Study

Blackthorn Information Security Guides a Fire Department IT Staff in Incident Response

The Client

A small city fire department.

The Scenario

The IT division of a small fire department initially suspected that they had pornography in multiple locations on the LAN, due to a large number of files which appeared to be porn movies according to the file names and extensions. Upon further examination, it was found that the files were spreading quickly throughout the network, in a manner very similar to a computer virus. To make matters worse, the same "porn files" had begun spreading to the LAN of the fire department's parent municipal government. While the client's IT was fairly experienced, they were unsure of whether they had employees intentionally hiding pornography in multiple areas on the LAN, or if they had a virus that their antivirus applications was not stopping.

The Investigation

Blackthorn Information Security was brought in to assist the IT staff in determining what exactly the problem was, and how to combat it. After examining the files, their various locations, and their contents, Blackthorn determined that the client's LAN was suffering from the spread of a "Trojan" program –software that hides abusive behavior by appearing to be a totally different type of program. The Trojan was spreading itself by a combination of three means: self-copying out to USB drives upon detecting use of a USB drive, tricking users' interaction to allow installation -triggered when users would attempt to see the contents of the "porn movie"-, and self-copying to all public folders on the network.

The Benefits

Blackthorn's investigation prevented unneeded or unfounded accusations, when it showed the fire department's IT personnel that the fire department employees were not storing pornography on the LAN. In addition, the IT staff was advised and assisted in fine tuning controls on the LAN limit such widespread contamination from Trojan programs in the future.