Case Study: Major City’s Municipal Courts

On Wednesday, February 4, 2009 a virus was discovered on the municipal court network of one of the ten largest US cities. The virus was initially thought to be the Conficker worm that was spreading through networks worldwide at the time, but was later determined to be a previously unknown variant of the Virut virus. This virus was not detected by anti-virus software. The virus infected about 475 of the city’s more than 16,000 computers, less than 3%.

As a result of the infection the municipal courts were shutdown from February 4th through February 13th. During the shutdown, police issued citations for some minor misdemeanors instead of arresting the suspects, as the arrests could not be processed.

Analysis

The relatively small percentage of computers affected and the large impact that resulted underscores the increased dependence we have on computers and information systems. While events such as these may be unavoidable, organizations need to understand the risks associated with these systems, and these risks should be managed in the same manner that other organizational risk is managed.

Staff should be educated about risky behaviors, such as opening attachments from unknown senders, that can allow viruses and other malware to propagate. And management must stress the importance of proper procedures when dealing with information systems. These systems are the core of most modern organizations and they should not be used without proper training.