Smart Dolphins
IT SOLUTIONS, INC.

White Paper

The Multi-layered Security Defense Against Ransomware

Due to the steady spread and rapid evolution of ransomware, Smart Dolphins has deployed a multi-layered defense against ransomware to improve the security and network stability of our customers.

The Rise of Ransomware

Ransomware is generally defined as malicious software that infects your computer and denies you access to your computer or files until you pay a ransom. Millions of ransomware infections are reported every year. Organizations today, require a multifaceted IT security program that is regularly evaluated and re-adjusted.

The Challenge

Smart Dolphins manages the IT networks of over 50 businesses, the majority of which are small businesses with limited resources for network security. Our challenge was to deploy an automatic multi-layered security solution across a large group of companies.

The first layer of our security approach includes these *six* essentials:

- Strong gateway security (firewall and routers designed to protect against ransomware)
- End-point anti-virus and anti-ransomware group policy settings
- Anti-malware DNS services
- Regular software patches and OS updates
- Rock solid backup and disaster recovery system
- Ongoing user security training

In early 2016, we added another layer of defense against ransomware. We now leverage the power of Microsoft's File Server Resources Manager (FRSM) to detect ransomware at work and stop its spread through network server shares. FSRM accomplishes this by stopping all server shares when it notices suspicious file access, thus stopping the ransomware from further encrypting file resources on the network. It also notifies us that an active infection has been found. By minimizing the damage ransomware can do, and ensuring that we become aware of infection promptly, business impact and recovery time can be greatly reduced.

While adding FSRM as a protective layer is a routine security measure, what is noteworthy is the automated, scalable way in which we have applied it. Without automation, we could not deploy it across our entire customer base and keep it up-to-date as new threats emerge.

Results

Since the implementation of these various layers of network security we have not had one threat across our entire customer base. Our approach to network security is proactive, as is our approach to all aspects of IT. We don't wait around for problems, but instead we have configured our computer solutions and network operations to greatly reduce problems before they happen.

If you are concerned about your organization's network security, contact us to set-up a free security and backup audit.