Direct Technology Battles Ransomware with 3-Prong Plan

Most companies never expect to be the victims of a cyberattack. But ransomware is insidious and undiscerning, striking even the smallest, most unlikely victims. Last year, companies lost almost $1 billion to ransomware. Recently, a Sacramento-area building restoration company experienced a ransomware attack that completely encrypted and locked down all of the business's files—many of which were not backed up. The company's leadership (who had experienced another ransomware attack two years prior) called Direct Technology after hours, and Direct Technology deployed an engineer immediately to the company site to diagnose and mitigate the problem. The engineer then worked with the company to develop a new strategy for backup and disaster recovery, as well as ongoing IT security and maintenance.

Upon arriving onsite, Direct Technology's first priority was locating the problem and preventing the virus from spreading further. The company had two servers, both of which had Dharma-encrypted files. The engineer recognized the virus as a variation of the CryptoLocker ransomware trojan and quickly removed network access for the servers and shut them down. From that point, the online security community took over searching for the ransomware encryption key, and Direct Technology turned its focus to disaster recovery and getting the company's employees back to work.

To that end, Direct Technology's engineer took the company's computers off the domain network, scanned them to ensure they were free of viruses, created local accounts for all users, and created a secure local network to connect them while a new domain network was being built. Because many employees were in the habit of saving documents locally, these measures allowed current work to resume with minimal disruption.

From this point, Direct Technology devised new strategies for recovery/replacement, backup procedures, and enhanced IT security measures.

Recovery/Replacement Strategy: The two infected servers will be kept aside until the encryption key is found, and Direct Technology has encouraged the company leadership to submit a case not only to the security community, but to the FBI. In the meantime, Direct Technology replaced the servers, firewall, and antivirus, and migrated certain data and processes to the cloud. The engineer also built the company a new domain network to reconnect computers to and reengineered their entire environment to be more secure.

Backup/Restore Strategy: Because the company did not have a robust backup strategy, most of the files stored in the servers since August 2016 cannot be recovered until the key is found. Upon discovering this issue, Direct Technology's engineer worked with the company leadership to devise a backup and disaster recovery strategy for the future, making recommendations for both new policies and equipment. If an attack or data loss happens in the future, Direct Technology will be able to restore and get the company back to work with less than a day of disruption.

Security/Maintenance Strategy: During the scan, the engineer discovered that the point of entry was an RDP account belonging to a company that the building restoration company had contracted work through. Though the company is small, it is clearly still a target for viruses. Because of this and other security/accessibility concerns, Direct Technology worked with the leadership to create a more robust security and equipment maintenance strategy. For example, the company reduced management access, requiring more people to call the help desk instead of attempting to make changes themselves—a more secure approach. In addition, leadership signed a maintenance agreement for a Direct Technology resource to periodically come in and provide care and feeding and general maintenance. Working together, these strategies ensure that policies remain consistently implemented and centrally stored.

Ransomware doesn’t only go after hospitals and governments and massive tech corporations. Without robust security and disaster recovery methods set up—and employees trained on DR procedures and knowledge transfer—ransomware can wreak havoc on any business. But with proper training and policies, and a plan to get assistance if an incident does occur, ransomware is a plague that can certainly be defeated.