Innovative Computing Systems

Case Study: Ransomware

Law Firm Ransomware Attack

Background

A well-respected 75-year-old law firm has been a managed services client of Innovative Computing Systems for more than 20 years. They had invested in antivirus software, but repeatedly declined to institute two-factor authentication at the firm, which has become a necessary best practice for data security in any industry.

Nefarious operators in Canada – using Russian software – gained access to the firm's systems via the administrator's workstation. They found a list of passwords on the administrator's machine, which gave them easy access to the information needed to launch the ransomware attack. Virtual and physical servers were encrypted, including the chipset on the servers, making it a very thorough attack. The firm uses VoIP, so even their phones were shut down. The firm's engagement with Innovative is such that they tried to handle issues in-house before calling in more resources.

Client
A small law firm with fewer than 50 attorneys spread across two offices in California and Nevada.

Challenge
An employee clicked on a link in an email sent by nefarious actors, unwittingly unleashing ransomware across the firm's servers.

Solution
Innovative Computing Systems' senior engineers were able to halt the attack, restore the firm's systems and get them operational within days.

Results
The firm now follows data security best practices and has launched data security training for all employees.

Solution

The attack happened on a Wednesday night. By Thursday morning, Innovative engineers were already involved. The team found that they needed to go onsite to make a connection into the network with a clean laptop to discover the scope of the attack. The firm had cyberinsurance, and the Innovative engineers worked closely with the insurer to verify the damage and rectify the situation.

Innovative engineers spun up stand-up virtual servers in the cloud, which the forensic team verified as infection-free. Another engineer worked on the switches, and determined they only needed to be rebooted, which brought the phone system back right away. The engineers also pulled the chipset out of the host servers and reformatted them. They then reinstalled the VMWare operating system. This was still a business day – with client work due, hearings for which to prepare and pleadings that needed to be filed by Friday. Because they used a document management system, they were able to retrieve the most important documents they needed for Friday by Thursday afternoon.

The firm had made hourly and nightly backups of their data. By Friday morning, the Innovative engineer had determined the point in time they needed to go back to in order to make a clean restore of all systems. All documents and emails were available by Friday at noon. Innovative engineers worked through Saturday and restored all firm operations – including 10 to 12 terabytes of stored data – by early the next week.

The firm lost a half a day of work, but with the work the Innovative team carried out, no ransomware was paid to the nefarious actors.

Lessons Learned

Had the firm implemented two-factor authentication as earlier recommended by the Innovative team, this ransomware attack would never have happened. Two-factor authentication now protects all entry points of access at the firm. In addition, the firm added Mimecast's Threat Protection, which looks up and verifies links in emails before they reach an inbox. They also added server-based software that detects attempted attacks. Finally, the firm does monthly testing and training with its employees to reinforce data security best practices.