Hospitals: Increasingly Popular Targets for Ransomware Attacks

4.5.2016

In recent days, hospitals in the Washington/Baltimore corridor have been hit by a spate of ransomware attacks, and there is no reason to believe that these attacks will not expand to include hospitals and other healthcare providers' systems elsewhere, including in Michigan. Indeed, US-CERT, the U.S. Government's Computer Emergency Readiness Team, has issued an "Alert" to warn hospitals and other healthcare facilities across the country of the growing threat. While cyber criminals have been using variants of ransomware to extort money for a number of years, the emergence of large-scale targeting of hospitals is a relatively recent development that is particularly pernicious. After all, the effects of a ransomware attack -- which infects a computer network and restricts access to it until a ransom is paid to unlock it -- can be, literally, a matter of life and death because such attacks can block access to the current medical records of critically ill patients. Ransomware attacks also threaten the continuity of operations of healthcare facilities, which could lead to even more horrific results.

In this case, a destructive ransomware variant, labeled "Locky," was observed infecting networks belonging to healthcare facilities not only in the United States, but also in New Zealand and Germany. Locky propagates through spam emails that include malicious Microsoft Office documents or compressed attachments, which contain macros or JavaScript files to download to Ransomware-Locky files. While some victims of ransomware attacks pay the ransom demand in the hope that the attackers are "honorable," there is no guarantee that the encrypted files will be released. Indeed, the only thing that payment guarantees is that the malicious actors will receive the victims' money, and in some cases, their banking information. Even if the infected files are decrypted, there is no guarantee that the malware infection has been removed.

Related Services

Cybersecurity and Privacy Specialty Team

Health Care

Health Care Industry Team

Privacy, Data Breach & Data Security

What Can Healthcare Providers and Facilities Do to Protect Themselves? While there is no product or service that will make a hospital's computer networks completely impervious to cyber attacks, US-CERT recommends that users and administrators take the following preventive measures:

- Employ a data backup and recovery plan for all critical information. The backup data should be kept on a separate device and stored offline.
- Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process.
- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting allows only approved programs to run, while blocking all others, including malicious software.
- Systematically install patches as they are released to protect your operating system and software with the most up-to-date code. Since most attacks target vulnerable applications and operating systems, vigilant patching will greatly reduce the number of exploitable entry points.
- The current versions of anti-virus software should be maintained, and all software downloaded from the internet should be scanned prior to executing.
- Restrict employees' ability to install and run software applications to minimize the number of unwanted programs and impeded their ability to spread within the network.
- Train employees to avoid enabling macros from email attachments, and install software that blocks email messages with attachments from suspicious sources.
- Report instances of fraud to the FBI at the Internet Crime Complaint Center.

In addition to following the US-CERT recommended precautions, Butzel Long also strongly recommends that administrators arrange cyber threat-avoidance training for all new hires and periodic training for all incumbent personnel; and that they update their employment agreements and employee manuals to specify that violators of cyber "hygiene" may be subject to discipline, up to and including dismissal.

If you have questions regarding cybersecurity requirements and best practices for healthcare facilities or providers, or other health care law matters generally, please contact your regular Butzel Long attorney, the authors of this alert, or any member of Butzel Long's Health Care Industry or Telecommunications and Technology Practice Groups.

Ira E. Hoffman
202.454.2849
hoffmani@butzel.com

Mark R. Lezotte
313.225.7058
lezotte@butzel.com