SBS institute
700 S. Washington Ave. Ste. 200
Madison, SD 57042

Holding Your Data Ransom

Written by:
Jon Waldman – Partner, CISA, CRISC - Secure Banking Solutions, LLC
Dylan Kreutzfeldt - Cyber Security Engineer - Secure Banking Solutions, LLC

What is Ransomware?

It's a day that starts just like every other day. You walk into the office, grab some coffee, and power up your computer. Only instead of being able to access your data, you see an image demanding you to pay $10,000 in the next 48 hours for the return of your data, or the price goes up. Today, it seems, won't be just like every other day; you've been victimized by ransomware.

Ransomware is one of the fastest growing methods of attack currently being deployed by hackers. From large organizations, like banks and hospitals, to medium sized retailers, all the way down to individual devices, such as personal cell phones, everyone is at risk.

Ransomware is a type of malware that will encrypt files and information on your organization's network, rendering your information (including customer records) inaccessible and denying access to other networked devices. Ransomware gains control of your organization's network through phishing emails, unpatched software, unsupported servers, and other vulnerabilities. Once ransomware has essentially rendered your network and information unusable, the attacker will demand payment in exchange for the encryption key and the promise of being able to decrypt your data once the organization has paid the ransom.

Who is this affecting?

As cybercrime has evolved into a business, hackers are now deploying ransomware as a new way of funding themselves. Cryptolocker, one of the first known versions of modern ransomware reported back in late 2013, infected thousands of computers before antivirus companies were able to update malware definitions in order to stop the attacks. In 2015, the amount of ransomware attacks grew by roughly 165%.

Some companies that paid the ransom found that the hackers did not provide the encryption keys or were unable to decrypt the data, leaving them without their data and or the money they paid in ransom. However, in many cases, hackers followed through on their promise to restore the data. Additionally, hackers frequently utilize "help desks" to assist with the ransom payment, often asked for via digital currency like Bitcoin, and even to help with the decryption of data. Since hacking has become a business, leaving victims without information and money does not help proliferate the scam; instead, hackers want you to regain access to your information, helping spread the word that paying the ransom is the best course of action.

In most of the organizations that have been infected by ransomware, such as the Hollywood Presbyterian Medical Center (which was forced to pay $17,000 US earlier this year), the clicking of malicious links in phishing emails was reported to be the cause of the breach. In the case of Hollywood Presbyterian, the hospital was unable to access email

or treat their patients due to the encryption of information and loss of technology-related services. The hospital's network was non-functional for ten (10) days, and some patients had to be diverted to other medical centers.

It is estimated that most ransomware attacks have gone undocumented after companies pay for the return of their data, in an attempt to protect public relations. There are ways, however, to mitigate the risks of ransomware affecting your organization.

How can I prevent this?

The most effective solution to ransomware is simple: ensure you have good backups. There are two types of organizations: those that back up their data, and those that wish they had backed up their data. If an organization employs a constant backup procedure that keeps backed-up information off the network, hackers will find their efforts in vain. If your backups are handled through a third party, be sure that you are performing proper due diligence to ensure that your vendor is taking steps to mitigate the risk of ransomware compromising your backed-up data as well.

Another way to mitigate risk is to be sure all software on the network is updated. Maintain a patch management program that regularly checks for updates for your systems and software. It is also good practice to delete any software not required for business functions.

Lastly, social engineering training and testing should be performed for all employees in order to teach them the dangers that exist in negligent computer use. Even the best antivirus software and firewall can't always help you once that employee has clicked that malicious link.

What can SBS do to help?

Secure Banking Solutions has a team of auditors and consultants that can assist you in developing sound Information Security Program practices, such as data backup procedures, patch management programs, and other risk mitigation strategies, as well as testing to ensure these practices are in place and working the way they should.

Additionally SBS has recently partnered with KnowBe4 to provide social engineering testing and training for financial institutions. If you are interested in performing your own internal testing and finding out how your employees will react to phishing emails containing potentially harmful malware, KnowBe4 makes this task simple and provides fast reports that are easy to read.

Contact SBS by calling 605-923-8722 to speak with one of our Help Desk representatives about our services. If you have any additional questions, comments, or concerns, please let us know; we are always happy to help. For more information, please visit SBS at: https://www.protectmybank.com/

Sources

http://www.cbc.ca/news/technology/hollywood-hospital-hack-ransomware-trends-1.3462062

http://betanews.com/2015/06/09/ransomware-sees-165-percent-increase-in-2015/