Idealliance

Bulletin
Idealliance Monthly News

July 21, 2017 • Volume 2, No. 7

Beware the Threat of Ransomware!

Cybercrime doesn't just happen to other people, and it doesn't just happen to big companies. According to Symantec, 50% of cyber attacks have targeted small businesses.

Idealliance Member Advantage Program partner BIZLock says that ransomware is the number one threat to businesses today and an attack can be very costly. But there are steps companies can take to help prevent having their—and their customers'—data being held for ransom.

"Ransomware is a type of malware used by criminals to encrypt your data rendering it unusable," notes BIZLock. "Since you need your data and software to run your business, you'll likely be willing to pay a ransom to the criminals to get your data back, that is, if you have no other choice."

The company cites two real claims to illustrate the threat. In one, a teenage hacker sabotaged a data network with Crypto-Locker type malware and demanded an extortion fee of $50,000 to unlock the company's own data. In another, extortion demands of $25,000 were made to prevent sensitive customer data from being released on the internet.

"Ransomware is an absolute epidemic with the malware and attacks spreading exponentially worldwide, in part, because malware and trojan viruses are easily spread by email (when someone clicks a simple link in a phishing email) and ransom payments being made via BITCOIN, which is essentially untraceable."

Into the Cloud

To best guard against ransomware attacks and avoid facing the prospect of having to do business with criminals, BIZLock suggests taking these five commonsense actions:

• **Back up your data, ideally into the cloud in real time.** This can be supported by having a simple secured backup drive in the office—not connected to the network and therefore not exposed to malware. There are numerous backup vendors, including, but not limited to, DropboxPro, MozyPro (Dell), CrashPlan Pro, Carbonite and Egnyte. BIZLock encourages businesses to work with their IT professional to make sure that whatever backup service is selected is in place and is tested regularly. "We've had too many instances whereby our clients have had backup that actually did not work as intended, thus resulting in significant loss," it cautions, emphasizing the need to test any system that is installed.

• **Use anti-malware, firewall, and anti-adware software** to better prevent phishing and trojan virus type attacks from reaching you and your employees.

• **Educate employees about the dangers of malware and ransomware.** "No one in your office should click on ANY email links that are from unsolicited/unknown sources," says BIZLock. "Because the stakes are so high, consider having consequences if they do."

Put Policy in Place

Developing and implementing a computer use policy is a best practice most companies are following. Although many businesses permit occasional personal use of computers it is a good idea to have guidelines in place and to enforce their adherence.

• **Update your computers with the latest patches**—98% of all successful attacks occur from vulnerabilities that are more than six months old!

• **Test your ability to restore from your backup.** "Unless you test the process, you are not ready to address the ransomware threat," notes BIZLock. "Literally, on a moment's notice, you need to be able to restore your computer operations or be prepared to suffer."

BIZLock® provides Idealliance members discounts on value-added consultancy services available before, during, and after a data breach incident, as well as cyber insurance in the event a breach occurs. Member discounts are available at ***https://bizlock.net/idealliance****. For additional discount offers, contact Idealliance's Tyler Keeney at (703) 837-1075. For members having annual revenues greater than $10 million, send your request and contact details to customerservice@bizlock.net. For members in New York, contact Ron D'Alessandro of Edwards & Company at (631) 472-8482. BIZLock is owned and administered by Identity Fraud, Inc., the national online cyber insurance program administrator for AIG.*