SMALL BUSINESS BIG THREAT

Ransomware: What you really really need to know

It is out there. A simple piece of code that launches another piece of code and begins a laborious process of changing your data from readable useful items to encrypted junk. It does not happen immediately and is insidious in its approach, eventually making all of your files unavailable to the most important person that needs them, you! Welcome to the always-scary always-unpredictable world of Ransomware.

In 2016, Ransomware attacks were up by over 167 percent and it continues to be big business with a take of almost a billion dollars a year paid out and countless others resolved independently, or not at all[1].

So what is Ransomware and should you worry about it? The answers are seemingly easy with the best being simply, "bad" and "yes". So let's look first at what Ransomware actually does.

When you are infected with Ransomware, your computer is altered as all files in your system are run through an encrypter. You may or may not be aware of what is happening, but as the files are encrypted they unencrypted files are deleted from your system. The net result is a computer full of encrypted data, with no access without a decryption key.

Early Ransomware often had mistakes in their approach, like leaving the decrypter key on the system[2] or having a telltale. Today, there is less likelihood of such as attackers continue to mature in the multi-million dollar industry. If you are infected you are far less likely to have an easy way out. Your net result will be a computer that cannot be utilized and your choices for being able to be effective again will be very limited.

The important question that everyone asks is "Am I at risk?". Many people like to think that a smaller business may not be at risk because it is not a big payoff. This is false as attackers are now profiting more off small businesses than larger businesses simply because the attack vector is easier. Why would an attacker spend days or weeks planning a big hit when multiple smaller hits can be relatively direct and payout as effectively since the possibility of encryption is higher? To put it simply, why attack one well protect group for $50,000 when ten $5,000 attacks pay the same.

Attacks can be even simpler than that. The shotgun style attacks can be on everyone, with the potential of infection equally distributed, but smaller businesses being the easier endpoint as they often don't spend the time or money to ensure their systems are protected effectively, and don't have the time to stay as engaged or as protected as the businesses with massive budgets and moderate workforces.

If you consider the big picture, it is very grim. Most businesses look at the picture and are so tied up in what might happen that they miss the big

[1] "2016 Saw An Insane Rise In The Number Of Ransomware Attacks" by Lee Matthews

[2] http://www.computerworld.com/article/2489311/encryption/cryptodefense-ransomware-leaves-decryption-key-accessible.html

AMERICA'S SBDC IOWA
POWERED BY SBA U.S. Small Business Administration
IOWA STATE UNIVERSITY COLLEGE OF BUSINESS

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

picture and end up doing very little to protect themselves or their users. If you are worried, and you should be worried, here are the things you should be doing right now!

1) **Review your Backup and Disaster Strategy:** Let us face it. Ransomware is a disaster. Even if you pay, you may not get a key to decrypt and may be patiently waiting for something that will never come. Since Ransomware effectively destroys your system, the only sure fire defense is to be able to restore that system quickly and efficiently. You might ask "But if I use a product, won't it protect me?" and the answer is "Sure, but you can always be one of the first victims and there would be no protection against that".

   A good backup strategy uses the 3-2-1 rule. Three copies of your data, 2 forms of media and 1 off site. Ransomware adds a caveat. The off-site backup cannot be readily accessible to your file system. More directly, the off-site backup cannot be a file copy to a service like Box, Dropbox, iTunes, or somewhere that just copies files. Why?

   We had a business call us just recently that was infected with Ransomware and used Box as a backup. They had a drive mapped and each night the files were copied from the server to Box. Guess what, when the Ransomware struck it encrypted all the backup files as well, leaving the business dead in the water, with no files at all.

   Also consider RPO and RTO. RPO is Recovery Point Objective or how much data are you willing to lose. As the amount of data loss approaches 0, the cost goes up for your solution. RTO is Recovery Time Objective or how long can you afford to be down. The closer this is to 0 downtime, the more cost goes up. Consider these two items carefully as most people will happily say they never want to go down and never want to lose any data, but the cost can be considerable.

   A good solution is something that may cost a little. There are super choices like Veeam and Datto that also offer cloud solutions. Datto even offers a temporary spin up host in the event of an issue. Other solutions are rampant, but there is a second part to having a good backup strategy, **test it!**

   If you end up attacked the solution then is easy, you restore to a point before the attack and avoid paying excessive amounts of money to restore your system.

2) **Train everyone:** The biggest threat to your systems is you and your people. In spite of all the stuff on the internet, if you do just your work and pay attention to how you approach internet communications your risk can be low, but how do you know how to avoid Ransomware when you are remote, on laptops, or all over the place in social media. We like to say common sense can work, but it only goes so far.

Education for your employees helps make them prepared to not fall for a Ransomware attack. A phish test (fake emails to groups to determine human entry points into an organization), more often than not, failed. This is simply because a single click or single entry is a fail for all.

There are numerous resources available and the SBDC does a great job of organizing these for small businesses. Take a moment and see what is right for you. There are also new products like KnowBe4 that will both train and test your employees at increasing levels of complexity. The goal of course is to stop the weakest link before that link can click and cripple you with Ransomware. Remember, the person you forget to train or skip may be the one that takes your systems down.

3) **Have protection:** There are many programs out there that can protect your system from some things, but not all of the threats will be handled by a single solution. There are also considerations to protect your network. Don't just go to your local store and buy what's on the shelf. Instead call in some help to layer a solution for you. At bare minimum get a good professional grade firewall (that means not one from a discount store), a good internet security program including virus and malware protection, and a good secondary protection program that blocks you from going places you shouldn't be going. There is always the chance of being patient zero, meaning there may not be a cure for something, but if you have a good structure, you will usually be safe. It is also a good idea to consider Intrusion Protection, email encryption, and password management to make sure you are even safer. No matter how you approach protection it is likely you should get help, simply because there is a lot to consider and it is not simply "one size fits all".

   We have run into several situations where people were guided to free or inexpensive solutions. As stated previously, consider the amount of impact any issue will have on your company and what that impact could cost before getting a free antivirus, or a cheap firewall, or just picking because of price. Pick because of features and need instead and you are more likely to be safe.

4) **Worst case, know who to call:** On the subject of getting help, know someone beforehand that can help you in that awful emergency you didn't see coming. All too many people think about the problem when it happens and struggle to find a solution. We recently had a customer come to us that had paid a huge sum of money to a company that was online for Ransomware recovery. After months they were told "sorry, we couldn't do anything" and all of their money was lost. In the first day, we recovered a score of files and helped begin the reset process. Find a company that is willing to help you set up, and will be there when you have an issue someday. This should be a company that has a proven track record of positive results across a variety of technologies.

Remember in the end your business is counting on you, your customers are counting on you. This is no longer a world where you can say that “it won’t happen to me” and instead it is a world online filled with dangerous people who want to take your money. Take a moment and consider how you could do your business without computers or access to the online world. Then take a moment and consider how much impact the loss of your systems will have on your bottom line, your operations, workers, and everything else it takes to make your business work.

Once you have done that, consider what it is worth not to lose that and the credibility associated with having Ransomware, or not being able to run your business effectively then react appropriately.

If you need assistance, reach out to the SBDC or find access to helpful resources that will show you a path towards avoiding Ransomware.

Of course, these actions are not all inclusive and there are more and more stringent procedures that can be taken. You need to decide how much you are willing to lose, and how much you might lose to make the best decision for your company. Make good choices and avoid seeing that lock screen on your system!

###