INFOPAYS
KNOWLEDGE IS THE KEY TO SUCCESS | JULY 2015

WHAT ARE "DATA RANSOMS"?

"It has become appallingly obvious that our technology has exceeded our humanity." Albert Einstein

Do you ever feel like technology is moving too fast for a small business to be able to keep up with it? If you answered yes, you are not alone. The pace at which technology advances today is a common pain point for the majority of independent business owners most of who are strapped for resources such as time and money that they can dedicate to this topic. And to make matters worse, technology opens up opportunities for fraud and different forms of data exploitation that can often be detrimental to a business. That being said, it has never been more important to keep informed about these trends and to be extra vigilant during everyday business.

In this edition of InfoPays we are going to review a form of malware called "data ransomware" -- an Internet virus that locks access to your computer files until payment (usually in the form of Bitcoin) is released. According to Wikipedia, data ransomware started circulating in 2013, and the way it starts is with an email that appears to originate from a legitimate financial institution but in it has a file attachment that is malicious and once executed, it infects the system with a trojan.

What can you do to protect yourself from this malware? The following five tips can help you minimize the risk of being affected by data ransomware:

1. Back up your data.

With this virus, data that is locally stored, as well as data that sits on mapped drives, can be both compromised. Making sure you can revert to an earlier state of your files is great relief in the case of blocked data access. Backups are often tedious to set up, but once they are in place, they are low maintenance and potentially life-saving.

2. Filter out emails that have executable file attachments.

Executable files usually come with an .exe file extension. Data ransomware has been known to install files through an executable file being run on the computer system. Making sure these files extensions are blocked from being seen as email attachments on your incoming email traffic prevents the possibility of human error and your employees being tricked into entering the scheme.

3. Patch and update software.

Outdated software can be another reason and an open door to any form of malware. Hackers target known vulnerabilities that

are exposed due to outdated software versions. You can either update your apps regularly or enable automatic updates if you prefer a more hands-free approach.

4. Have proper security systems and practices in place.

Ensure that you have a firewall that comes from a reputable provider as well as a solid anti-virus program installed company-wide. Malware creators usually release newer versions to avoid people catching on with the scheme. Having both a good anti-virus/anti-malware software on top of a good firewall ensures that even when the anti-virus/anti-malware misses any malicious software due to newness, the firewall can still catch it.

5. Keep staff informed.

Perhaps the most important point is to make sure staff is aware of these trends, and in this particular case anyone who deals with financial institutions should be vigilant about not becoming the next victim of data ransomware.

The core lesson that comes from all this, however, is to perform regular data backups. Maintaining good file backup systems becomes more expensive and time consuming as a business grows, but if done properly it can save your business life. That's at least one thing that we can be thankful for when it comes to data ransomware -- it makes us take our data backups seriously.

Source: www.welivesecurity.com

STRATEGIC PLANNING

"Study the past if you would define the future." — Confucius

Conventional wisdom reflected through axioms such as "If it ain't broke, don't fix it" may work well for some aspects of your business, but not work well for your strategy. Strategic planning is a dynamic process that involves minute-to-minute awareness of our surroundings and an ability to move fast, all while remaining stable. We are already halfway through the year, and as another year nears, we are getting you started with ideas and tips on how to approach your next strategic planning exercise:

1. What business are you in?

Know which business you are in. Know your competition well and know your market even better.

2. What other businesses are you in?

Try to see your organization through a wide lens—in which other businesses are you involved or have the potential to get involved? Expanding your service or product is an excellent opportunity on which you can capitalize.

3. What are your core competencies?

You core competencies are what makes you different in the market. These are the activities that make your product or service unique and allow you to grow. Unlike activities you outsource, core competencies are things you can perform better than others could on your behalf and are much more than mere strengths.

4. What are your core values?

Know what values you stand for. Are you oriented towards operational excellence at the expense of minimizing customer service expenditures? Or do you value investing in customer relationships in order to gain long-term, passive growth?

5. Which, if any, competitor will be your next partner?

Your competitors can become allies if you ever consider strategic partnerships -- make sure you maintain good relationships.

6. Are your short-term goals and long-term strategies aligned?

In order to maximize shareholders' capital, most organizations adopt a quarter-to-quarter mentality. Look beyond the quarter to align your short term visions with your long-term profitability goals. Good strategy means asking the right questions and asking them often. Know your business model assumptions, be thorough and keep your strategy under constant scrutiny.

Created by the IPS Business Owner Success School (BOSS)