Ransomware and How to Protect Your Company

by

Scott Augenbaum

It’s fair to say that “Ransomware Attacks” are on the rise. Sadly, Ransomware is not a new issue.

I had a 20+ year career with the Federal Bureau of Investigation (“FBI”) and over the last decade of my tenure, we provided guidance to the public on this topic…..yet it still remains a critical issue.

In 2019, I spoke at the InfoSec Conference in Las Vegas and my co-presenter, a retired FBI Agent then working for a major intrusion response company, affirmed to the vast audience that Ransomware was at epidemic proportions. I noticed a number of folks in the crowd were rolling their eyes (in disbelief) at his statement.

To be honest, as recently as 2019, very few companies were taking the Ransomware threat seriously.  A common chain of thought questioned why would anyone want to target them or their organization. I would especially hear this time and again from nonprofits and religious organizations. Make no mistake, Cybercriminals do not care who you are or what kind of business you run. Even a church can be targeted. Here are a few examples of how severe the threat is:

* In 2021, the Cybercriminals targeted the Washington D.C. Police Department. To make matters worse, the Cybercriminals claimed that they would release some very sensitive information to the public if their demands for compensation were not paid. This was not the first time the Cybercriminals made the point that if they can encrypt your data, then they can also steal it.
* The Colonial Pipeline incident showed that Cybercriminals have the ability to shut down a major portion of our country’s critical infrastructure. The tools and, dare I say instructions, to commit these crimes are all available on the Dark Web.
* In May, JBS Foods, one of the biggest meat processing companies in the world, paid an $11 million ransom demand. This is one of the largest Ransomware payments of all time.
* Over the 2021 July 4th weekend, approximately 1,000 organizations around the world were affected by a Ransomware attack on the U.S. information technology firm, Kaseya. The Cybercriminals realized that by attacking one organization, they can impact a large number of other companies throughout the world.

During my decades with the FBI, I discovered that by the time law enforcement is alerted of a Cybercrime/Ransomware incident, the FBI cannot come to your organization quickly enough to wave a magic wand that will fix the problem. Since most of the Ransomware perpetrators are located overseas, it is equally challenging to bring these evil doers to justice. I know that these two points alone cause a lot of anxiety.

But the good news is that things are not hopeless. My biggest epiphany while I was with the FBI was recognizing that a majority of Cybercrime incidents could have been prevented.

Is Ransomware prevention easy? The answer is no. However here is a quick list of steps you can take to reduce your chances of becoming the next Ransomware victim.

* Realize phishing is the number one attack vector for the distribution of malware. You will get an email, a text message or even a Facebook message asking you to click on a link or to open an attachment.
* You can get infected if you go to a questionable website or a website that has been infected with malicious code (This is called drive-by malware).
* Make sure your computer/smartphone/device is updated to the latest operating system and that all applications are patched. Do not ignore your device when it says it/software needs to be updated.
* Reduce your attack surface on your device. Only allow trusted applications to run on your device. Beware of all those free software products that you never use. (This is called application whitelisting).
* Reduce administrative rights for other users. Administrative rights allow other users to install programs and malicious code on your hardware. If your device asks you to enter your password to install or make changes to a program, you need to be careful.
* Take an inventory of who you are allowing onto your network and what they can they are allowed access. Does the employee from three years ago still have Administrative rights to your network? You do not want (or need) to allow every employee to have access to everything on your network.
* Use two factor authentication on all remote access to your network, especially remote desktop protocol (RDP).
* Backing up is not enough ... make sure you test your backups and have a good restoration plan. Remember, if your network is infected with Ransomware there is a good chance the Cybercriminals have also stolen your data.
* Educate yourself and your employees about the dangers of Ransomware and Cybercrime.
* Contact your local FBI Office if you are a victim or go to [WWW.IC3.GOV](http://www.ic3.gov)

Finally, here is an excellent resource from the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA).

<https://us-cert.cisa.gov/ncas/alerts/aa21-131a>

This information from the FBI can be helpful as well to establish best practices to protect your company:

<https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

About the Author:

The author is retired FBI agent Scott Augenbaum. In 2003, Scott was promoted to Supervisory Agent in the FBI’s national headquarters in the Cyber Division, Cyber Crime Fraud Unit, where he managed the FBI Cyber Crime Task Force Program and the FBI’s Intellectual Property Rights Program. In 2006, Scott transferred to Nashville and managed the FBI Memphis Division Computer Intrusion/Counterintelligence Squad.

He is the author of *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime.* https://cybersecurityventures.com/14-cybersecurity-tips-from-a-former-supervisory-special-agent-fbi-cyber-division/