SOCIUS
CYBER BYTES
VOL 0.1 _ 2017

The Wannacry CYBER ATTACK and How to Avoid Falling Victim to the Next Attack.

By: Laura Zaroski, J.D., RPLU Socius insurance Services

The WannaCry ransomware attack was a worldwide cyber-attack by a ransomware cryptoworm which targeted computers running certain Microsoft operating systems. The attack encrypted the data and then the attacker demanded a ransom payment. Within a day of the attack, it is said to have infected more than 230,000 computers in over 150 countries. Shortly after the attack began, a web security researcher discovered an effective kill switch found in the code of the ransomware. This greatly slowed the spread of the infection, effectively halting the initial outbreak 3 days later. But don't get comfortable - new versions have since been detected that lack a similar kill switch.

Wannacry made big headlines because it spread around the world so rapidly. It infected computers from all sorts of industries as well as personal computers. Based upon how successful Wannacry was at infecting so may computers in such a short time, industry experts are certain that there is good incentive for copycat attackers to repeat such an attack, and to make it even bigger and better the second time around.

As no one is 100% safe from experiencing a breach, businesses should anticipate and prepare for a breach. Vulnerabilities can come from many directions, so organizations should constantly monitor and protect their networks to avoid being any easy target. Hackers are crafty and ever diligent in designing new ways to get you to click on their malware. A popular way to attack is to apply tracking software to your computer and to monitor the sites that you visit. Then, the hackers craft an email that appears to come from one of your trusted vendors (shopping site, banking institution or government entity, etc.) in hopes of getting you to click on an attachment from that source. BINGO! They are in...

How do we prevent and protect against "Wannacry2" or "Wannacry-the-Revenge"? The best strategy is to implement good cyber hygiene. Good hygiene includes installing updates as soon as they are released. Don't let cyber attackers exploit known vulnerabilities in existing software and then walk right into your systems. Make sure you are backing up for files outside of your network. Much of the new ransomware finds the backups FIRST, and makes sure to corrupt or encrypt those files before locking down your system. Finally- and most important- is the human error factor. Train your employees to be on the alert for suspicious emails and to NOT click on fishy attachments. Social engineering scams are only getting more sophisticated – so your workforce needs to get more sophisticated too! Cyber experts advise that new ransomware appears every day. Many of the strains are available for purchase on the internet and can be deployed even by the most un-tech savvy users. Think before you click!

The security policies and procedures of an organization should be customized around the demands and the types of threats facing that organization; not every organization will experience the same threats. To determine the vulnerabilities facing your organization, it is important to perform risk assessments that will expose potential vulnerabilities and that will help minimize cyber risk.For example, have an outside firm perform penetration testing so that you can identify your weaknesses and address them before an attacker takes advantage of them. Contingency and disaster recovery plans must also be in place so in the event of an attack, the organization can react effectively and immediately.

TAKEAWAY:

Wannacry should serve as a BIG wake-up call for companies who have yet to assess their cybersecurity status and to update their practices and systems. It is time to prepare for the next round of attacks. And they will come... There is no doubt that companies of all shapes and sizes, will continue to fall victim to the similar but likely more advanced ransomware attacks.

As the stakes continue to get higher, your cyber risk analysis and contingency plan should include a well-tailored cyber insurance policy. Be ready when the inevitable happens! Prepare your workforce and systems for the next attack! And purchase a robust cyber policy that will be there for you in your hour of need.

www.sociusinsurance.com