protiviti®
Face the Future with Confidence

This Weekend's Ransomware Attacks – What Your Company Needs to Do

May 15,
2017

The attacks that took place around the globe this weekend were not new, but had a greater, wider-spread effect than ever seen before. The attacks leveraged ransomware (a form of malware which encrypts data and files and demands payment to restore access to them) and may have been made possible through leaked tools from the National Security Agency (NSA) in the United States. The malware took advantage of a previously disclosed Microsoft vulnerability, for which many systems have not yet been patched.

What Happened?

Reports indicate the attack struck hospitals, companies and government offices around the world, with the majority of the attacks targeting Russia, Ukraine and Taiwan. It disrupted computers that support factories, banks and transport systems. The National Health Service in the United Kingdom was attacked, causing some surgical procedures to be cancelled and ambulances to be diverted. In addition, several major global companies reported they were hit by the attack, which currently is believed to infect more than 200,000 computers globally. Targeted entities have been told to pay ransom with untraceable online currency.[1]

We may never know the full scope of the attack, as many firms may not reveal they were victims and whether they paid ransom. Among those companies that did report the attack, some noted that, in responding to it, they were forced to shut down entire systems in order to slow the spread of the virus. The source of the attack has not been identified. And, sadly, the attack may not be over. Bottom line, we could be looking at an escalating threat.[2]

Ransomware attacks have been used before and attacks that exploit Microsoft vulnerabilities are not new. So why did this attack have such a profound impact? The fundamental reason lies with organizations continuing to either ignore or not effectively respond to the issue and, as a result, failing to modify their security programs to combat these and other evolving threats on

[1] "Global Ransomware Attack: 5 Things to Know," Laura Smith-Spark, CNN, May 13, 2017, available at www.cnn.com/2017/05/13/world/ransomware-attack-things-to-know/.

[2] Ibid.

an ongoing basis. They skirt the immediate attack at hand and feel fortunate they were not a victim of the attack. Thus, they fail to apply the lessons that others have painfully learned.

These attacks reinforce a harsh reality: Cyber attacks not only are about data loss or intrusions on privacy, but they also are more likely to impact organizational operations, patient care (for healthcare providers), critical infrastructure and possible loss of life. To make matters worse, systems that support critical operations – such as medical devices and industrial control systems – often run on older technology that is more vulnerable to these attacks. These operational technology networks are typically not patched and maintained as well as traditional corporate information technology networks.

What Should Companies Do?

It is time to recognize that ransomware and more sophisticated cyber attacks are a very real threat that will continue and likely will become worse and more frequent over time. Attackers have been emboldened by the successes they have achieved through these attacks. Organizations must realize cyber defense is not a mere checklist, a one-time project or an effort that ends with reaching a certain milestone. Cyber defense is a never-ending process of improving internal systems and capabilities to guard against rapidly evolving threats.

Organizations must look at operational technologies such as medical devices and industrial control systems to design adequate defenses which protect and maintain these technologies. They must recognize that focusing on critical data assets and information systems – the so-called crown jewels – will not address ransomware threats. Accordingly, they must reassess their risk assessment process to ensure it accounts for impacts beyond just data loss and privacy intrusions. Exposure to ransomware is an example of an adverse business outcome or scenario that must be managed to ensure that enterprise security solutions are more comprehensive than steps taken based on a narrower focus on specific assets and systems. That is why organizations should evaluate their cyber incident response plans to ensure they are up to date for new attack types and that IT security personnel are trained on how to respond.

Following are key actions organizations should take immediately:

- Conduct an inventory of systems within the organization. Organizations cannot protect systems and networks they do not know they have.
- Ensure all systems and applications are patched and up to date.

- For critical technologies which cannot be patched (e.g., medical devices, industrial control systems, legacy applications), implement mitigating controls to protect them, such as network segmentation and other solutions.
- Continue to support a culture that promotes security and security awareness among employees. Ensure that employees receive training on ransomware threats on an ongoing basis.
- Revisit cyber defenses to ensure the program addresses the risk of ransomware. Confirm the organization has updated information on indicators of compromise (IoCs) for recent attacks.
- Ensure the risk assessment process considers cyber threats more than once a year. Because threats are evolving so quickly, the risk assessment should be performed quarterly for new threats and risks. In addition, the risk assessment process should consider risks beyond just sensitive data loss. Other risks, such as operational impacts and disruption, could be affected through cyber attacks. Design appropriate cyber defenses to mitigate these risks.
- Ensure the organization has a sound, up-to-date incident response plan that considers new threats such as ransomware. Conduct training and rehearsal of this plan through simulations (e.g., tabletop exercises). The plan should be revisited more than once a year – ideally, quarterly – depending on the risk to the organization.
- Review organizational business continuity and disaster recovery plans. Ensure these plans are up to date and include recovery procedures for business disruption due to a cyber attack.
- Ensure cyber defenses are adequately funded and staffed to manage the evolving risks and threats.

Summary

This vicious global attack is just another example illustrating that cybersecurity remains center stage as a top risk for companies as they increase their reliance on new technologies in executing their strategies. Many are referring to it as a "wake-up call" and that's exactly what it is – for governments, companies, software vendors and policy makers.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®