Energy Company Devastated by Petya Attack

The Attack

On a Sunday in early July of 2017, a form of ransomware slipped through a Google Drive document and brought down a major us-based energy company with thousands of employees. Normally when attacked by ransomware, as the name suggests, a demand in the form of payment is required in order to retrieve the stolen data, but this case was different.

In late June there were various reports of a new wave of ransomware attacks, referred to as a slew of different names including Petya, exPetr, Petrwrap, and NotPetr. After further investigation it was determined that while the virus demanded a ransom once it had infected a system, it was unable to determine the user paying the ransom so this virus is really a wiper disguised as ransomware. It takes your money, and still destroys your data. Although they are some of the rarest kinds of malware, wipers are incredibly destructive and have seen a spike in occurrences in recent years.

At-a-Glance

Industry: Energy

Business Impact: Within 24 hours, ½ of the company's 250 hosts were rendered un-bootable by the virus. The only way they could stop it was to turn their entire data center off. More than 3 weeks later only 60% of operations were restored.

Lessons Learned: Move to current operating systems and keep them patched. Educate users on the risk of consumer cloud services and their use in the enterprise. Make sure your team has a fully documented disaster recovery plan and it is practiced at twice per year.

The Assessment

Attacks were concentrated in Eastern Europe and Ukraine in particular. A business in the energy sector was attacked by the virus not long before this incident and was written about in the European media. Then a few weeks later, through a shared Google Drive with the business, the virus leaked and wrought havoc on the company's servers. Due to the fact that the victims were using Windows 2003, a very outdated operating system, the patching was not in place, vulnerabilities were everywhere. With no disaster recovery strategy in place, the company was brought to its' knees from a data storage standpoint.

The way this particular virus destroyed data is by rebooting the machine, then while it looks like it is running a check disk utility, the virus was encrypting the file location tables, rendering all of the file data on this file system useless. The company had 250 servers, and in 24 hours half of them were rendered un-bootable by the virus. Once the virus sunk its teeth in, they couldn't stop it and had to turn their entire data center off. For about a week, half of the company's servers were shut off while the environment was sterilized and secured. Because of the way this virus was transmitted, there was no way of telling who or what had been infected, so each piece of data needed to be looked at individually and be cleared before shutting them down again. Once that process was complete, the data recovery process could begin.

The aftermath of this attack from a simple leak in a Google Drive was nothing short of devastating. Everything was shut down for a week: no email, no progress, and no new data. Only after about a week or so was the company able to turn on a few key systems but most of the web-hosting data was lost completely and needed to be recovered. Three weeks after the attack business is operating at about 60% of their infrastructure with the remaining 40% needing to be rebuilt or recovered.

How could this have happened?

It's no secret that there are evil people all over the world, and some of them get their kicks out of attacking businesses through viral attacks. Businesses and individual users sometimes understand these threats and take great precautions and preventative measures to prepare, but this Energy Company was nothing short of a sitting duck on a freeway. The month long ordeal and recovery process from the attack really started before that Sunday in July with an extreme lack of preparation and an outdated disaster recovery strategy, if you can call it that.

With only a few hodgepodge solutions, including a snap-shot based technology that was only used for patch checks, a backup server that was not patched at all or maintained properly, and a tape-based disaster recovery strategy, the data infrastructure was no match for this malware attack. Shortly after disaster struck, this company reached out to SIS to assist in the recovery and to help sort out the colossal mess on their hands.

Since the back-up server was not patched and maintained, when it was hit it was lost. "The main problem was that their disaster recovery techniques were outdated. They were using the old method where you need to reload the operating system, re-deploying the backup software, then restoring from a tape… They then found that their backup process for rotating tapes would overwrite some useful tapes because they didn't have enough window of protection…" according to Jeremy Brovage, a Storage Architect with SIS.

The attack was on a Sunday, but their last database backup was on the previous Friday. So on Saturday and Sunday new tapes were being generated but there was no way to recover the data from those tapes. Jeremy and the SIS team were able to get to a recovery point of Friday where the last backup was, but lost everything generated on Saturday and Sunday.

Steps your business can take

While the SIS team continues to work on repairing the damages from the attack, there are ways that this company, and really any company can bounce back quickly and efficiently. First, it is important to have the newest and most up-to-date operating system. Whatever operating system you are using is patched and serviced properly, regardless of whether or not it is the most up to date. Newer operating systems have updates that remove potential vulnerabilities where potential malware attacks can occur.

There's a famous saying that says most battles are won or lost before they are fought, and in the case of disaster recovery this is 100% true. Make sure your company has the most up-to-date operating system, develop a disaster recovery strategy, and have an expert you can call when disaster strikes.

About SIS

SIS is a total technology solutions provider serving more than 1,300 customers nationwide. Partnered with leading IT vendors, SIS delivers hardware and software solutions, technical expertise, consulting services and data center solutions. The company's Managed Solution Center is a state-of-the-art Tier 3 data center facility that provides comprehensive hosting and cloud offerings, including virtualization, business continuity, security, storage management and application support as well as systems monitoring and management. Founded in 1982, SIS is headquartered in Lexington, Ky. and has regional offices in Indiana, Kentucky, Michigan, Ohio, Virginia and West Virginia. For more information, visit www.ThinkSIS.com.