tracesecurity
Compliance, simplified.

White Paper

The Rise and Absent Fall of Ransomware

Kevin Ivy

TraceSecurity Security Solutions Engineer

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Executive Overview

On Saturday mornings, especially in the Spring and Fall, I enjoy grabbing a cup of coffee, the newspaper, and heading to the back porch for reading. The newspaper is usually loaded with random stories from world news, local news, local and national sports, classifieds, deaths, and burglaries. Burglary-related articles typically catch my attention because not only can the stories be crazy sometimes, at least where I live, they can also alert on trends in a particular area.

For me, reading through these types of stories can elicit feelings of thankfulness or relief, because it wasn't me or didn't happen to me. This happens throughout life when we see things happen to other people or businesses. So much so that we get into a mindset that there is no way that it can happen to us for a multitude of reasons such as "we have the most secure network," "we are in the middle of nowhere," and two of my favorites: "it has never happened before" and "we are a small fish in a big pond!"

In this time of rapid technology growth and conversion from physical data to digital, there is an adverse, negative effect that has risen - the growth of cyberattacks. Each day, organizations around the world are reporting breaches of their data. What is the number one reason for these breaches? The infamous Ransomware attack.

By looking at the world, it can sound like some slap together Hollywood movie, but it isn't related to that at all. In fact, it has rapidly emerged as the most significant cybersecurity risk to organizations in our nation! We know Ransomware isn't a Hollywood movie, so what is it?

What is Ransomware?

Ransomware began gaining traction in 2012 and has grown exponentially since then due to the increase in the number of successful breaches. It is essentially a type]of malicious software, or malware, that locks users out of their computers, servers, tablets, laptops, smart phones, and many more gadgets. In addition to being able to lock devices, it can also lock files or business data. The problem is that the only way to unencrypt the devices or files is by paying a ransom to the attacker in hopes that they provide the encryption key needed to undo the damage. If victims are not willing to pay the ransom, they can rely on data backups or be prepared to start over from scratch.

Ransomware is a huge problem that fails to go away due to the number of successful attacks, especially involving the use of spear phishing. Spear phishing is the most successful method of injecting Ransomware into a target's network and it is accomplished by sending emails that contain malicious links or software to specific individuals or departments within an organization that appear to be from a reputable source. Once the user falls for the phishing email and clicks on the attachment, for example, the Ransomware malware begins encrypting files on the machine and then pivoting to other devices on the network, if possible.

Per Cyber Security Ventures, "A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021." The Baltimore City government is the largest entity to make the headlines in 2019 after being hit by a Ransomware attack. In addition to crippling the city's government for over a month, the attack cost them an estimated $18 million to recover from. The worst part about it is that attackers only demanded $76,000 to be sent to them via Bitcoin. So, we know that Ransomware is a real threat to American businesses, the damage caused by them is detrimental financially, and that it isn't going away any time soon!

Reducing Risks

By now, we should have an understanding of what ransomware is and its adverse effects on an organization. The best strategy is to get ahead of the attacks by reducing the likelihood of their occurrence and implementing a plan should one occur. There exists no way of completely shielding businesses from ransomware attacks, but there are preventative measures that can be taken to reduce the chance of it happening. Let's go over some of those:

Security Awareness Training

Having a secure infrastructure, while integral to business functions, does little to solve the human element of an IT network. Any business is only as secure as the employees who help maintain it. While there are many platforms and solutions available on the market today, we will cover some basic procedures to establish a security-minded workforce.

The first step in the right direction is establishing procedures for employees to attend training on common security topics that they will face in their industry. This instruction can be provided in person or online in a digital class. The next step is, of course, to ensure that the newly created procedures get established and that all new employees adhere to it. Once the initial training is completed, establish a periodic training plan to include management and executives, and adhere to it.

Backing Up Data

The number one step to recover from a Ransomware attack is restoring data from a backup. To do that, businesses must first have a well-tested and consistent backup plan in place. Identify all the critical data in the environment that the business would not be able to function without and include it in the backup plan. Also, identify all critical systems and ensure that they are backed up as well. Determine a backup frequency that fits the business's needs and budget and stick with it. Backing up data more frequently reduces the overall gap in time when a restore must be relied on for accessing data and systems after an impacting event.

Next, utilize off-site backups to reduce the chance that the backup data is affected during an incident. Many cloud solutions offer secure transmission and storage of backup data. An essential item to discuss when choosing an off-site backup solution is how long it will take to restore if business data has become corrupt, encrypted from a ransomware attack, or affected by any other event. It's great to have a detailed backup plan that includes cloud storage, but if restoring vital services takes an extensively long time, the restoration process can be just as crippling as the attack itself.

Lastly, testing backup processes regularly and identifying a routine schedule will ensure that the procedures and solutions are working as they should. There is no worse situation than having a Ransomware attack lock all of a businesses' files, and when restoration from data backups is attempted, the business finds out that the backup jobs are corrupt and have been for some time. All of these factors are why it is key to establish a backup plan, execute the backup plan, and test the backup plan.

Least Privilege

Exercising least privilege for a company as a whole can be a huge undertaking upfront, but it is very beneficial in the securing of data and eliminating excessive access by only giving users access to what they need to do their jobs. In addition to users, the principles of least privilege should also extend to software applications and services that run in an environment. Without exercising this principle, a successful Ransomware attack could inflict much more damage if all of the accounts and applications on the network have full access throughout. For example, if Linda in accounting only had access to the applications and file shares that she needs to perform her job, a successful Ransomware attack may only be able to affect those resources.

A great way to start implementing this principle is by grabbing a sample from a department, identifying everything that they use on a regular basis, locking down their accounts to only those items, implementing those levels of access into a security group to be applied to the rest of the department, and moving to the next department. It will not work perfectly at the beginning so expect trial and error, but once the initial implementation has been completed, it should just become an ongoing process that should be evaluated on a regular basis.

Patch Management

Patch management is one of those tedious tasks in IT that can have a love-hate relationship with IT staff. We love it when everything goes well and hate it when nothing works like it should, right? Regardless, it is one of the top ways to further secure an environment and the devices operating within it. For most businesses, the word "device" can mean many things, such as servers, workstations, laptops, mobile devices, routers, firewalls, IoT devices, and many more. As vulnerabilities are discovered on these devices, vendors and developers typically release patches to remediate them.

To develop an adequate Patch Management program, we must be sure to include all those devices because leaving any device unpatched on a network can increase the chances of a successful attack. The easiest way to start is by inventorying all the devices connected to the network regularly. Once all devices have been identified, procedures for handling both Operating System and third-party application patches should be developed. Depending on the size of an organization, patches can be managed and applied manually or handled with a solution such as Windows Server Update Services (WSUS).

There are many solutions today that can make an organization's "patch management" life bearable and much more manageable. Regardless of the method, determining the best time to check for patches and then applying them regularly is crucial to ensuring that this process does not affect business operations. If budget allows, it is best to test out patches in a separate test environment before rolling them out to the production environment to minimize the chance of a disruption in business functions. The most significant difference between a lackluster patch management program and a great one is staying on top of the latest patches and sticking to established schedules.

Incident Response

The best way to prepare for an incident is to have a plan in place that has been tested and agreed upon by internal stakeholders. The National Institute of Standards and Technology (NIST) has published the Special Publication 800-61 that provides guidance on handling incidents. NIST is an excellent industry-agnostic resource that can be used to assist in creating an organization's Incident Response Program. This standard for handling incidents follows a four-stage life cycle: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-incident Activity.

The "Preparation" phase is the most time-consuming phase because it is where the specifics of the entire plan are created including defining an IRP team, how to handle different types of incidents from identification to mitigation, the roles of responders, notification procedures, and much more. Additionally, it is also the phase where the business should ensure that all staff has been trained on the documented procedures and that the plan has been approved by management.

The "Detection and Analysis" phase is where the incident response team monitors the environment to determine if an event should be treated as an incident. The "Containment, Eradication, and Recovery" phase is first focused on containing an incident once it has been identified. Determining how the incident occurred and remove any of the attacker's remnants or backdoors to ensure that further damage isn't caused is essential to this process. The Recovery portion is where backups and recovery plans are utilized to restore data and systems, if necessary. The last phase, Post-Incident Activity, is where all the incident response procedures that were implemented in the actual incident are reviewed to see if there are areas for improvement.

Security Testing

A great way to test out an organization's defense mechanisms and overall security is through the different types of security testing. Since most Ransomware attacks primarily gain access to networks through social engineering attacks such as phishing emails, these simulations are very valuable. With that said, two of the most popular types of security testing are penetration testing and social engineering.

Penetration testing is an exercise that primarily targets networks, internal and external, and sometimes targets business applications. The goal for these engagements is to find vulnerabilities and attempt to exploit them to see what data or systems can be compromised or manipulated. Don't waste time on automated tools or software that claim they can perform thorough penetration tests. Through my personal experience with penetration testing, I have gotten to points during testing engagements, where it isn't possible programmatically to do so.

For example, while performing a penetration test, there are times where information gathering and reconnaissance is key to furthering an attack and being able to make real-time decisions based on that information can oftentimes be the distinguishing factor between a successful and unsuccessful attack. Technology and A.I. have advanced but have not yet surpassed what the human element can provide in this testing.

The next type of security testing is Social Engineering. Social Engineering is a broad category of testing because it can be performed onsite or remotely, and each approach has its perks. Onsite Social Engineering is typically where an actor will go to a business's location and pose as an employee or a local vendor in an attempt to gain access to sensitive areas. The purpose is to test employees' adherence to established visitor access and escort policies.

Remote Social Engineering is the most popular security testing that I see performed at most organizations. Just like Onsite Social Engineering, it uses impersonation for its attack, but instead of being in person using props and disguises, it uses fake emails, SMS messages, and even phone calls.

The number one method used in successful Ransomware attacks is email phishing. A phishing email can disguise itself as someone trustworthy in an attempt to deploy malware or gain sensitive information, such as usernames and passwords. Since it is such a highly successful attack vector, all businesses should be running simulated email phishing campaigns to test their staff regularly.

There are many security firms and solutions that provide phishing campaign services and solutions, so it just comes down to what fits the budget and exact needs, but at the very least, something should be done. Since phishing attacks account for 90% of all data breaches and the average financial cost to recover from these data breaches is $3.86m, regularly testing the staff through simulated email phishing campaigns should be a priority. With executives being the most targeted individuals at businesses, it is important that they are included in these simulated phishing campaigns as well.

Recovering From An Incident

Businesses can do everything possible in terms of preparing for an attack and securing their business data, but it is impossible to remove the risk of something happening altogether. So when that something does happen, we need to know how to respond and recover. Here are a few simple steps to take:

Incident Response

The first step to take once an incident, or more specifically, a Ransomware attack occurs, is to initiate the Incident Response Plan. In the last section, we briefly discussed what this is and what an ideal plan should contain. Now it is time to put that plan to the ultimate test - a real incident. Since the incident has already been detected, the next logical step is to contain and eradicate the attack to reduce the total amount of damage caused. With the primary goal of Ransomware attacks being to encrypt or lock as many files as they can and hold them ransom, the quicker the attack is halted, the fewer files or data that will potentially be lost, for now.

Assessing The Damage

An attack was successful, and some data has been encrypted, so what's next? Go through the entire environment to determine what has been affected and what hasn't to know how to approach recovery and specifically, what needs to be recovered. One thing that can be forgotten when frantically trying to sift through the rubble is connections that touch our networks such as third-party vendors, business partners, and customers. Knowing that Ransomware attacks can spread, it would be beneficial for all parties involved to take measures to ensure that they haven't been affected. Once the total damage has been assessed, it is time to initiate recovery efforts based on prioritization from business impact assessments.

Restoring Data

Now it is time to start restoring the systems and files that were encrypted during the Ransomware attack. If a well-tested backup plan (like mentioned above) has been established with persistent backups, restoring data and affected systems may take some time, but the amount of file or data loss should be minimal. However, if a business has skimped out on their backup plan due to unknown reasons, restoring data could set them back a bit. That is why it is fundamental to any business to ensure that adequate backup schedules are performed to reduce the overall risk of data loss or system downtime.

Lessons Learned

The attack has come, data and systems were encrypted, the Incident Response Plan was initiated, the damage was assessed, and data and systems were restored. Everyone can finally breathe a sigh of relief because it's over. However, it isn't over yet! Now is an excellent time to review how the business handled the incident per stated policies to identify how they can better improve the policies and procedures going forward. In addition, identifying how the attack was successful and looking for ways to reduce the chance of re-occurrence is vital. Whether it was Linda clicking on a phishing email or John giving his username and password over the phone, identifying the cause is critical. There is no one-button fix-all solution. However, ensuring that well-tested procedures are followed, having staff trained, and building a hardened environment can reduce the risk of an attack or recurrence.

Unfortunately, Ransomware isn't going anywhere for the foreseeable future due to ever-evolving techniques. The best that we can do is to properly prepare for it as businesses and if we fall victim to an attack, do our best job at containing, mitigating, and recovery from it.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.