There has been a lot of news lately about new strains of ransomware such as Petya, WannaCry, NotPetya, GoldenEye, CryptoLocker, etc. I wanted to send this email out to you to ensure that you have a clear understanding of today's threats and how to best protect your environments from not only the ransomware reported by the media but also the unknown threats that your organization may be exposed to.

What's unique about Petya, NotPetya, and WannaCry? These are the strains of ransomware that have been getting a lot of media attention recently. The scariest characteristic of this type of malware is that, once one system on your network is infected, it can spread from one system to the next very quickly and autonomously. No further user interaction is required. These ransomware variants make use of a vulnerability in Microsoft's file sharing protocol, "SMB", that allows the infected system to easily infect other hosts on the network. If you allow file sharing then your network may be vulnerable to these infections and they may be able to spread across this network very quickly. You may be at risk of being locked out of systems and losing all data on infected devices. You can prevent infections from spreading by ensuring all your systems are patched against the vulnerability [MS17-010].

Ransomware is just another form of malware and you can protect yourself the same way as from any other type. It doesn't matter what name it's been given or if it's received lot of news and media attention. Malware is a piece of unwanted software on your system that has harmful or damaging effects. You can Maximize your protection against all types of malware with a layered security approach. There is no silver bullet, but you can do a lot to ensure you're maximizing your protection against these threats.

The approach at a high-level is:

1. Prevent the infection from occurring. If you can, ensure that your users and systems do not get infected to begin with.
   a. Ensure all your systems are fully patched (including 3rd party applications that windows update doesn't cover)
   b. Harden systems
   c. Use technologies to prevent download or execution of unwanted code
   d. Monitoring and alerting to ensure you're aware of possible infections
   e. Educate your users

2. Minimize damage to the infected system.
   a. Employ all forms of the principle of least privilege

3. Prevent spreading of the infection to other systems.
   a. Network segmentation and firewalling
   b. Use technologies to prevent spread of known infected files

4. Clean up and recover after an attack or infection
   a. Perform regular on-line and off-line backups
   b. Have a Disaster Recover and Incident Response plan
   c. Regularly test your plans to ensure there are no flaws. Be ready!

LCM Security has hands-on, practical experience in deploying a complete security strategy for many organizations across Canada and the United States. I've prepared the following list of recommendations that I would highly advise you to review in case there are certain items that you have overlooked within your organization's security strategy. LCM Security works with organizations of varying size and with diverse budget requirements; the list is organized to balance cost and security effectiveness.

Detailed approach to maximizing your protection against security threats:

1. Conduct a security assessment:
   - You should evaluate where you stand as an organization. This exercise can be done by in-house staff, or with the help of one of our security specialists. Either way you choose carry this out, be sure to use a proven methodology that educates you on your security holes before someone else discovers and exploits them. Security Assessments by LCM Security provide you with a security score, relating your security stance to similar organizations; and, most importantly, groups your security gaps into a series of manageable projects that you can undertake at your own pace.

2. Run vulnerability scans regularly:
   - Internal and External Vulnerability Scanning is crucial. You want to ensure that all your systems are patched and hardened. It is extremely common for organizations to assume that windows patching is all they need and to forget about all of the third party applications that are usually not patched via windows update i.e. Java, Adobe, Browsers. There are also situations where windows updates fail to install, or additional registry edits may be required to secure a system. The goal is to make sure that you know where the flaws are every system in your environment so that they can be remediated. Running regular vulnerability scans will give you this information, which you can then use to analyze and prioritize your efforts accordingly.
   - With respect to the latest ransomware, a vulnerability scan such as this would tell you which systems are vulnerable to the SMB exploit that allows the ransomware to spread across your network.

3. Use technologies to prevent download or execution of infected code:
    - Technologies can be deployed either on the endpoint that you're trying to protect or at the network level that include:
        - Antivirus/antimalware
        - Intrusion Prevention System (IPS)
        - Access Control Lists
        - Botnet protection
        - IP Reputation
        - Application monitoring
        - Denial of Service Prevention
        - Web Filtering
        - File Integrity Monitoring
        - Web Application Firewalling
        - Sandbox analysis
        - Anti-Spam/Phishing
        - Data Leak Prevention
        - 0-day virus detection methods
    - The ability to inspect encrypted traffic (SSL) needs to be considered with the deployment of these strategies. Traditional deployment methods are unable to see encrypted traffic and become ineffective without this ability.
    - There are a lot of technologies that can be used to help protect your environment. Deciding which ones to deploy is determined by the result of your security assessment and budget-vs-risk analysis.

4. Educate your users:
    - One of the largest threats to an organization is their employees and users. It's imperative that users are aware of today's dangers and are trained to recognize potentially harmful behaviour.

5. Monitoring and Alerting:
    - Awareness is key. Knowing what systems are in what state, what is happening on your networks, and being able to find anomalous events. Set up automated alerts and monitor for anomalous activities in order to have complete visibility into what is happening in your environment. LCM Security offers services to deploy SIEM technologies to be managed by your team or by our Security Operations Center (SOC). Regardless of your budget we have a solution that will provide the right level of visibility into your network.

6. Prevent or minimize the damage and spreading of infections/attacks:
    - It's important to always use the principle of least privilege to minimize who has access to what. Network segmentation and positioning security devices between network segments plays a large role in preventing the spread of infections. Your ability to detect 0-day malware and prevent It from spreading further is another high importance item that should not be overlooked.
    - This is an exercise that involves ensuring the network architecture is optimal and the correct security technologies are deployed in the most effective locations on the network. Authentication mechanisms play a very important role in the principle of least privilege and the use of central authentication is recommended.

7. Be prepared to clean up and recover:
    - Ensure you have a backup strategy for your most important files. If you fall victim to a ransomware attack your data will be irrecoverable without backups; unless you pay and are fortunate enough to be dealing with an “ethical” criminal. Aside from backups, you should have a disaster recovery and incident response plan to ensure you’re not in complete panic-mode during a crisis. You want to be able to follow a guideline and take the right steps in the right order to get you back on your feet. These plans and backup strategies need to be tested on a regular basis to be sure that they work as expected and that they can be executed correctly and in a timely manner.

LCM Security can help you with any or all of the steps involved in having a sound security strategy. We help with the discovering of the holes within your organization, developing a plan with you to address them, proposing technologies to implement, assisting with implementation of those technologies, providing vulnerability scanning, and helping to remediate and recover from an incident.

I will wrap things up with a single piece of advice to you: run your vulnerability scans regularly (at least once per quarter is recommended), and make sure everything is patched!

If you have any questions or would like to know more details about our services feel free to give me a call or send me an email.

Piotr (Peter) Swoboda
Director of Engineering
LCM Security Inc.
Canada: 1-416-213-0224 x116
USA: 1-770-417-5894 x116
Email: pswoboda@lcmsecurity.com