A Best Practice Guide to Mitigating

Ransomware in Your Enterprise

Introduction

One of the most lethal forms of cyber attacks, ransomware, can disrupt the most powerful institutions in the world, from government organizations to Fortune 500 companies. Ransomware is a type of cyber attack that gains control of your system and holds it for ransom by encrypting data.

Ransomware typically tries to make its way into an enterprise's network via phishing websites or emails. Say an unsuspecting user opens an attachment, the ransomware launches itself, infects their system, and encrypts their files and folders, or even their entire hard drive. It then demands a ransom amount to be paid in bitcoin within a deadline, after which the data is permanently encrypted. Hackers use bitcoin because it is a digital crypto currency that ensures their identity cannot be traced.

The biggest problem with ransomware is the dual nature of the malware that it uses for the attack. The malware not only encrypts your data, but also is a worm that can spread across the network, affecting all the systems in an enterprise. This lateral movement is done by exploiting reported or unreported vulnerabilities. For instance, WannaCry and Petya ransomware use the EternalBlue exploit in Windows to quickly spread across an enterprise's network.

Combating Ransomware

While threat intelligence vendors work tirelessly to give security analysts more insights into cyber threats and quickly come up with solutions to detect and mitigate attacks such as WannaCry and Petya, it can take them time, anywhere from a few hours to a few days to analyze the working of any ransomware attack. Meanwhile, if your enterprise is vulnerable to the attack and if you don't have proper security measures in place, there is a high chance of your organization falling victim to the attack.

However, there are certain safety measures that can help you protect your network. Here are the 4 simple best practices that you can implement to prevent ransomware attacks in your enterprise:

4 Best Practices to Guard Against Ransomware Attacks

1. Educate your users on cyber threats
2. Secure vulnerabilities and passwords
3. Backup your data
4. Security auditing and alerting

1. **Educate your users on cyber threats:** Ransomware intrudes networks through phishing. A naive user may download a seemingly legitimate attachment and unknowingly infect their system. And even if most users are aware, all it takes is one user to be infected, as WannaCry and Petya make use of a Windows exploit to spread across your network, taking down even the most careful user's system.

   So, making all users in your enterprise aware about security risks and the dire consequences of an attack is a must. Start by telling your users to exercise caution while visiting unknown websites and opening mail attachments from unknown sources. This itself can go a long way in the prevention of an attack.

2. **Secure vulnerabilities and passwords:** Vulnerabilities in your network are what attackers use in order to carry out cyber attacks. Identifying and fixing these security flaws is fundamental to mitigating threats and securing your network. This includes regularly applying patches provided by your software vendors that ensure your systems are secure.

   In the case of WannaCry, Microsoft released a fix a month before the attack happened, and yet hundreds of thousands of systems worldwide didn't have the latest patch. It is a must to ensure all your systems are running the latest versions of software and you aren't using any defunct OS such as Windows XP. Also, make sure that your privileged account passwords are protected and administrators have strong passwords because this is what hackers seek in order to gain full control over your network.

3. **Backup your data:** One of the most important things that experts re-iterate is to NOT pay the ransom amount as that only encourages hackers to create a market for 'ransomware as a service'. So, it is vital for you to ensure your critical data is backed up periodically so that in the event of a ransomware attack in your organization, you can reformat your system and reload your data. This ensures that in a worst case scenario, not only is your data is safe but you also don't have to pay the hackers.

4. **Security auditing and alerting:** A SIEM (Security Information and Event Management) solution can audit security events occurring across your network and correlate them to provide actionable data, helping you to instantly detect and mitigate ransomware in your enterprise. With a SIEM tool, you can be alerted for system events associated with ransomware installation such as process or service creations. You can track suspicious activities on your file servers such as several file modifications occurring within a short period of time and also detect the creation of a ransomware encrypted file in your network. A SIEM tool makes you proactive in responding to threats by automatically executing a custom script to fight the attack immediately upon the alert getting triggered.

Using the latest cutting edge security applications including threat solutions and a SIEM tool to unify security information will equip your security operations center with the visibility needed to combat ransomware and other cyber attacks.