Ransomware Protection Plan

NotPetya ransomware holds the record for being the most devastating cyberattack in history. With a price tag of 10 billion dollars in damages and attributed to a state actor it is unparalleled in impact and cost for recovery.

A single piece of malware/code that paralyzed global corporations, brought ports to a halt, government agencies to their knees during the outbreak.

And massive impact on global economy and insurance companies in its aftermath.

As Atlanta and Texas make news in this arena, there are two important facts to know:

Ransomware is not going away, not anytime soon.

Ransomware is avoidable.

Ransomware is a type of cyber attack where information is held hostage for a ransom. The most common ways for it to enter a system is through email or as a result of visiting certain websites.

It has become more rampant in the past year and continues to intensify. Why? Because the returns are good, so it's a good return on investment for bad actors.

AND

Because it's easy to hide the tracks and increase the chances of getting away.

These returns are getting better as seen by offerings such as ransomware as a service, RaaS. Like other cloud based service offerings these offerings allow latest versions of the software and tools with a easy delivery model. What that means is the skills required to create and conduct the attacks are available thus reducing the price and barriers to entry even further. The recent ransomware attacks on the city of Atlanta and Texas involved SamSam, a RaaS. These attacks are are unleashed on targets and probe them for vulnerabilities, and once they get in they proceed by escalating privileges to wreak damage by encrypting files for higher impact.

Ransomware distribution kits such as Jokeroo, Cerber, Grandcrab have been available on the darkweb for years. RaaS will add even more to the velocity and frequency of Ransomware attacks.

Impact on Business

Ransomware has the potential and has been known to cripple business, in particular those that are not prepared. Companies need good backups to survive ransomware, but its critical to know these attacks are all about access. If the backups are accessible on a compromised network, they are vulnerable to the attacks as well.

Strategy for resilience

Comprehensive inventory of all mission critical systems and applications:

- Versioning information,
- System / application dependencies,
- System partitioning/ storage configuration and connectivity, and
- Asset Owners / Points of Contact.

Access control

Continuously review centralized file share access-control lists and assigned permissions.

- Restrict Write/Modify/Full Control permissions when possible.

Monitoring

Audit and review security logs for anomalous references to enterprise-level administrative (privileged) and service accounts.

- Failed logon attempts,
- Privilege escalation,
- File share access, and
- Interactive logons via a remote session.

Patching

Have an alert process for getting updates for security from vendors for assets in the organization

Monitor and assess the integrity of patches and AV signatures which are distributed throughout the enterprise.

System and Application Hardening

- Ensure that the underlying Operating System (OS) and dependencies (ex: IIS, Apache, SQL) supporting an application are configured and hardened based upon industry-standard best practice recommendations. Such as Utilize role-based access control.

Network Segmentation

Ensure that centralized network and storage devices' management interfaces are resident on restrictive VLANs.

- Layered access-control, and
- Device-level access-control enforcement – restricting access from only pre-defined VLANs and trusted IP ranges.

Educate employees

Like other malware, ransomware often infects a system through email attachments, downloads, and web browsing. Organizations should conduct regular training to help employees avoid common malware pitfalls.

Conduct regular data backups

Conduct regular backups of your system and store the backups offline and preferably offsite so that they cannot be accessed through your network (For ransomware, offline is more important. For other events, offsite is more important).

Verify the data backup process to ensure backups are capturing all necessary data and that the restore process works in your environment.

Restrict code execution

Restrict execution of ransomware from temporary and data folders, via access control.

Restrict administrative and system access

Some strains of ransomware are designed to use a system administrator account to perform their operations. With this type of ransomware, decreasing user accounts and terminating all default system administrator accounts can create an extra roadblock.

Maintain and update software

Another important yet basic rule for protecting against and/or ensuring early detection of ransomware is to maintain and update software, in particular security and anti-malware software.

Next Steps: Ransomware is preventable but there is no silver bullet, no technology that by itself will make you immune to it. The most important protection for companies is to assess their current state of vulnerability and assess the scope of impact. The solution is not a point solution but one that provides greater and broader security - one that includes people, process and technology.

Pamela Gupta recently posted this on Ransomware "You cannot have a strategy to protect the brain if you cannot keep the body healthy. Ms. Gupta is a security thought leader with more than twenty years of experience in creating strategic security programs in large complex implementations and environments. She has provided security guidance for development of large scale software and systems. She has also architected security for multi-million dollar secure networks and applications with various levels of trust. This involved developing Secure Application design, architecture and process And creating training aimed at educating developers and management on ways of achieving Security & Privacy by design.