LBMC INFORMATION SECURITY

Ransomware Preparation Checklist

Ransomware attacks are very difficult to defend against. There is no single control you can deploy to ensure you are protected. However, there are several things that you can implement together to help prevent or detect these attacks. When deployed properly, the following security controls can help reduce the risk of your organization falling victim to a ransomware attack.

☐ MATURE & TESTED DATA BACKUP PROCESS

A data backup is a quick way to recover from a ransomware incident. Performing regular backups ensures that a current backup of your data will be ready at a moment's notice. Additionally, regularly testing backups is an important step in confirming that the backup will provide a successful recovery. Because ransomware has the ability to infect mapped network drives, it is recommended to store your data backups off-line in a secure location.

☐ VULNERABILITY AND PATCH MANAGEMENT PROCESSES

Many variants of ransomware are delivered via phishing emails or exploit kits. Regularly scanning your assets is vital in identifying and patching vulnerable applications, such as Adobe Reader, Adobe Flash, and Internet Explorer. In addition, SamSam is a type of Ransomware which exploits vulnerabilities found in unpatched JBoss applications. A superior vulnerability and patch management process will ensure that all internal and external hosts are not vulnerable to these delivery methods.

☐ IMPLEMENT PRINCIPLE OF LEAST ACCESS FOR NETWORK FILE SHARES

Ransomware has the ability to propagate and encrypt data on mapped network drives. Limiting the privileges that users have to network file shares will also limit what the ransomware is able to encrypt. This helps to ensure that the infection of one user will not result in the loss of the majority of the data on a file share.

☐ APPLICATION WHITELISTING

This will allow trusted software to run while preventing unknown software, such as malware, from running. This additional protection does not rely on antivirus signatures and can prohibit malicious email attachments or online downloads from running.

☐ IDS/IPS WITH THREAT INTEL

Detecting ransomware events in real-time will enable a quicker response from your team, limiting the time that the ransomware has to spread. The blocking capability of an IPS

provides an opportunity to block communications to the command-and-control servers dead in its tracks.

☐ BLOCK TOR AND I2P TRAFFIC

Some of the latest variants of ransomware communicate with their command-and-control (C2) servers using the TOR or I2P networks. Blocking access to these anonymous networks will prevent the ransomware from communicating with their C2 servers and may thwart the ransomware from fully installing.

☐ DISABLE ACTIVE CONTENT IN MS OFFICE FILES

MS Office files with malicious macros are often used to perform an initial ransomware infection. Ensure that active content is disabled by default, and train users not to click the "Enable Content" button unless they are 100% certain the file is not malicious.

☐ SIEM USE CASES

Monitoring system and application log files for indicators of ransomware attacks can allow you to identify attacks early and possibly contain them. The following items are examples of ransomware indicators that a SIEM can identify (list is not exhaustive):

- Binaries running from %AppData% or %Temp%
- Execution of PowerShell Scripts
- Use of VSSadmin.exe
- Registry: HKCU\Software\Locky\pubkey
- Registry: HKCU\Software\Locky\id

☐ BLOCK UNCATEGORIZED AND UNKNOWN WEBSITES

The overwhelming majority of the time, the first level of ransomware delivery is from either a phishing email or drive-by download. In both instances, the exploit ransomware is housed on a temporary Internet web server that is not categorized, unknown, or newly registered. Therefore, blocking access to these types of websites will greatly reduce the ability for the ransomware to be downloaded to infect the machine while the devices are on the corporate network. This step will also build stronger protections against most other malware types. This step could potentially cause issues and should be tested and monitored before implementation.