THE ULTIMATE CHECKLIST FOR

Ransomware Attack Prevention

In response to the ever-growing ransomware threat, our Senior Security Analyst Tony Robinson has put together a list of action items you can use to keep your enterprise secure.

What is ransomware?

Ransomware is a type of malicious software that blocks access to data or systems until the requested ransom is paid. The reality is, ransomware is causing major damage to organizations and it's only going to continue getting smarter and faster.

Ransomware often spreads through mass phishing techniques–tricking users to click on a malicious email with weaponized attachments, but it also spreads through vulnerable software, malvertisements, exploit kits, and removable media (e.g., USB drives).

Proactive security can reduce your ransomware risk

PHASE 1: EMPOWER USER AWARENESS THROUGH EDUCATION

Protecting your networks through proactive measures often starts with your employees. To improve workforce awareness, having some degree of user security awareness training to help prepare your employees with best practices is an important step.

What should you consider when creating your **User Security Awareness Training**?

- [ ] **Context is key.** Help your users understand how security is relevant by incorporating relatable connections to their working and personal lives.
- [ ] **Clear definitions.** Not only should you explain related attacks, but you should include any related technical jargon as well–and all acronyms should be written out. Not all users are familiar with what words like "phishing" mean.
- [ ] **Reinforce actions.** Depending on company culture, this might mean incentivizing user awareness. For example: users who report a phishing email receive a $10 Starbucks gift card.
- [ ] **Easy reporting.** Provide employees with an easy way for them to report something suspicious to your IT/security team. Set up an email alias or group system for quick communication.

  Note: Some emails can be configured with a "Report Message" button that will auto forward the email to the security team or an automated solution to investigate before sending it to the team.
- [ ] **Emphasize "trust, but verify."** Encourage critical thinking among your users. Teach users to question everything as well as keep in mind that if something sounds too good to be true, it probably is.
- [ ] **Build a positive community.** Users will be more likely to cooperate if their feelings about security

PHASE 2: CONFIGURE EMAIL AND SYSTEM SECURITY CONTROLS

Below are great tips for the overall security system, including and especially email, to prevent other ways ransomware can (and probably will) be installed. Implement these 10 technical controls to catch malicious documents trying to sneak into your system:

- [ ] **Disable macros where possible.** Disabling Office Macros is one of the best ways you can start maintaining a better level of control over your email security.

  Note: Before taking this step, determine if/how macros are used in other departments to avoid any issues. Also, disable macros on files downloaded from the Internet.

- [ ] **Turn off the Enable Macros option:** It's important to note, many phishing attacks leverage the Microsoft Office default settings by luring users to click on an "Enable Macros" button.

- [ ] **Consider digitally signed macros.** Especially if disabling macros isn't an option, digitally signed macros will be the next best step.

- [ ] **Change default file associations.** Ensure commonly abused file formats are configured to avoid execution when double-clicked.

- [ ] **Block specific file types or attachments.** It's important to block commonly abused file formats at the email gateway. Also, consider investing in solutions that can analyze compressed files (7z, rar, zip, gz) for malicious files.

- [ ] **Implement an email quarantine.** This will require users to confirm the legitimacy of legacy document file format or macro-enabled documents.

- [ ] **Utilize blacklisting solutions.** A couple examples you can check out are SenderBase and Spamhaus.

- [ ] **Implement a Sender Policy Framework (SPF).** SPF is an email validation system designed to detect and block email spoofing.

- [ ] **Configure external email messages with tags.** For example, messages received from third parties will have "[External]" in the subject line. You can also implement the addition of a red bar popup at the top to draw a user's attention to the subject line and indicate they should exercise additional caution.

PHASE 3: SEGMENT FILE AND NETWORK ACCESS

Bottom line: Every user should not have access to everything. The process to implement these security controls surrounding your file and network permissions sharing may take some effort, but when it comes to avoiding the consequences of a ransomware attack, it's definitely worth it.

- [ ] **Limit local administration access.** Again, general users should not have access to everything–and especially not to local admin access–unless there's a very good reason. It is recommended to provide the minimal amount of access required to conduct their work-related activities.

- [ ] **Create a user-friendly access request procedure.** This type of documentation will help alleviate any employee fears of taking away too much access. Sometimes access is kept just in case, and this helps eliminate that issue.

- [ ] **Restrict file permissions and network share permissions.** Only authorized users should have permissions to make changes. Ransomware is getting smarter and can enumerate net shares.

- [ ] **Template roll-outs.** Even though this is one of the more challenging security controls to implement, once it's completed, the user role and group templates are easy to roll out.

- [ ] **Implement network segmentation.** If ransomware does in fact enter your network, there should be minimal communication between networks to prevent/minimize spreading. Partitioning a network into smaller subnetworks improves control and security against threats like ransomware.

- [ ] **Consider a Windows Firewall integration.** A lot of self-replicating & semi-self-replicating malware relies on Server Message Block (SMB) (e.g., 139/tcp, 445/tcp) to be opened between peers to spread. Denying SMB access between peers puts a stop to a lot of the malware from being able to move laterally.

- [ ] **Review access frequently.** A review should take place monthly or quarterly, depending on organization user amount. The purpose is to ensure those who need access do, and those needing to be removed (e.g., people no longer working there) will have access removed.

  Note: It's important to have a procedure for deleting user accounts upon their leaving the company.

PHASE 4: CREATE A SOFTWARE RESTRICTION POLICY

It's important to prevent unauthorized applications and other software from running on your network. Here are a couple things you can do to avoid this becoming an issue.

- [ ] **Set up Software Restriction Policies (SRPs).** Application whitelisting (explicitly allowing the use of certain apps) is something to consider when determining role-based access control. Once you determine which apps are being used, you can then set up SRPs to allow ONLY these to run.

- [ ] **Intermediary Step: Utilize cryptolocker SRPs.** As a go-between step, you can use the cryptolocker SRPs and block execution from @WINDIR@\temp\,%APPDATA% and %LOCALAPPDATA%. Test before deploying!

PHASE 5: USE ALTERNATIVE APPS AND BROWSER HARDENING

Using alternative apps where possible is an easy way to boost your security. Check out Ninite for a list of free applications, as well as a great solution for deploying them.

- [ ] **Standardize on an alternative web browser.** Some of your options here include Google Chrome and Mozilla Firefox.

- [ ] **Enable pop-up blocker.** Deploy either browser with an ad blocking add-on, such as uBlock Origin. This will prevent URL redirection attacks to malicious pages.

  Note: uBlock Origin is an ad-blocker that also functions as a popup blocker, but they are not always one in the same. Be sure to choose what fits best for what you want and need.

- [ ] **Disable frequently exploited software.** Adobe Flash and/or Java web plugins are a couple that come to mind. If you must use Flash and Java, make sure they're up-to-date.

- [ ] **Utilize Internet Explorer (IE) Administration Access Kit.** If you must have IE, and Java Web and/or Flash, consider using this kit to restrict access to only those sites where IE is required.

- [ ] **Incorporate a built-in, view-only PDF reader.** If users only need a PDF reader for viewing, both Chrome and Firefox have a built-in PDF reader you can use.

- [ ] **Investigate alternative PDF applications.** If users require the additional ability to digitally sign, fill out, and/or print PDFs, consider investigating apps other than Adobe (e.g., Sumatra, Nitro, Foxit).

PHASE 6: PRIORITIZE PATCH MANAGEMENT

Regular patching ensures your software is free of holes and eliminates the entry points hackers and ransomware. Applying security updates can go a long way in avoiding the spread of ransomware in your systems.

- [ ] **Update regularly and prioritize patching.** As soon as releases are available, you should update your operating system (OS), web browsers, and office applications. If prioritizing is necessary, select applications that interact with the Internet to be updated or patched first.

  Note: In certain instances you may not want to update immediately, unless it's a high severity update. System administrators may prefer to test patches first–in a corporate environment or giving time to analyze how it will affect the application being used (e.g., in some environments, updating Java may break the entire VM infrastructure).

- [ ] **Determine mitigation steps when patching is not available.** Read the patch notes. Determine the potential impact to your network. Find out if there are mitigations that can be used in lieu of patching. If not, determine the criticality of the issue and submit a change control to patch issues in order of criticality as soon as possible.

- [ ] **Identify applications and programs you do not need.** Eliminating apps and programs you don't use minimizes the number of updates as well as the amount of potential zero-days (vulnerabilities with no patches available).

  Example: Browsers are not necessarily needed on a server with a purpose not involving surfing the web.

- [ ] **Be proactive by staying aware.** Stay up-to-date on the latest detection, definitions, and fixes. If you can't patch, you can at least have the ability to detect attacks and remediate as necessary. Ensure you're following the resources that regularly release security updates

  Examples: Full Disclosure Mailing List, Google's Project Zero, TippingPoint's Zero Day Initiative, and your vendor newsletters.

PHASE 7: IMPLEMENT BACKUPS AND A DISASTER RECOVERY PLAN

Last, but definitely not least, it is critical in the world of information security today to ensure your backups and disaster recovery plans are in order.

- [ ] **Set up multiple redundant backups.** Use offline backups when possible, even if the offline backup is an external harddrive you purchased from Wal-Mart. Test to confirm backup method performance.

- [ ] **Ensure secure access control/management.** If backing up to a Network Attached Storage (NAS), a Storage Area Network (SAN), or a cloud solution, ensure strict access control–only those directly responsible for backups should have access, passwords securely stored, and 2FA used.

- [ ] **Run disaster recovery (DR) exercises.** Running DR exercises, such as simulated ransomware preparedness tests, ensures your failover (backup/restore) procedures work correctly.

- [ ] **Run a backup rotation and scheme.** Determine what's best for your environment, set it up, and make sure to test the integrity of the backups periodically.

- [ ] **Visit NoMoreRansom.org.** As a last ditch effort–prior to paying the ransom–visit NoMoreRansom for available decrypters for the ransomware you were attacked with.

  Disclaimer: Paying the ransom often results in making you a bigger target–there's no guarantee paying will result in returned data and/or they may simply come back for more.

- [ ] **Backups are your last line of defense.** Backups should be used as an alternative to paying the ransom. It is recommended that you never pay the ransom, because there is no guarantee the data will decrypt properly.

How Hurricane Labs can help

Hurricane Labs' dedicated SOC can help you implement the appropriate strategies for your enterprise environment. Contact us to learn how we can help strengthen the weak spots in your security and prepare you for a

P. 216-923-1330 | 888-276-4106

E. sales@hurricanelabs.com