Potential Ransomware Preventions and Cybersecurity Insights

CATIC IT Security

Cyber Hygiene – *Scans*:

Ransomware does not start with automatic encryption of files, it starts with overlooked access, exposure, and lack of training. A potential start to combat a ransomware attack is to start with the reduction of your attack surface. In other words, ransomware does not "just happen," as threat actors will deliberately comb through known vulnerabilities and weaknesses to plan their attacks.

It is best to begin with **web** and **vulnerability** management scanning services to pinpoint certain public-facing exposures you have, along with outdated applications both on the web, local, and cloud levels. Vendors that dominate the web and vulnerability management area are as follows:

- Tenable/Nessus.
- Burp Suite Enterprise.
- Rapid1 InsightAppSec.

Besides enterprise-grade solutions, there are various free tools that can be utilized by companies. As with most free products, there is a chance that you will be missing robust features, but it is a modest alternative to not having any product in place:

- OWASP ZAP.
- OpenVAS.
- Nikto.
- CISA (Cybersecurity and Infrastructure Security Agency).

CISA's scanning services require a no-cost enrollment, in which you provide information about the company/domain(s) in question. It can take a few days for an initial response, and results can take up to two weeks to produce.

Cyber Hygiene – *Email Security*:

While threat actors will conduct long reconnaissance efforts to find vulnerabilities that they could take advantage of externally, it is far easier and more efficient to simply "hack" the human. Nearly 90% of all successful cyberattacks start with a phishing email, which can act as the initial step in launching ransomware. In 54% of these cases, ransomware will be unleashed from the phishing email's malicious downloads, Office files, etc.

Some notable players in the email security realm that can help thwart ransomware are as follows:

- Mimecast.
- Proofpoint.
- Barracuda.
- Microsoft Defender for Office 365.

Steps to consider and potentially take with email security for your environment can also include:

- Disallowing certain attachments from inbound emails that can contain malware (e.g., .rar, .exe, .msi, .scr, .vbs, .bat, .docm, etc.).
- Enact geoblocks on your spam filtering, which prevents certain countries from emailing your users.
- Have IP blacklisting/reputation checks in place.

- Turn on URL re-writing (if possible) with your provider. URL re-writes will scan links in real-time for potential malicious activity.
- Implement anti-spoofing and impersonation policies.
- Have inbound/outbound malware scanning for all emails.
- Add banners to inbound emails that can flag suspected impersonation messages and look-a-like domains.

Cyber Hygiene – *Network Segmentation*:

Practicing network segmentation can offer a barrier in ransomware's plan to pivot laterally across your networks. Reasons for considering network segmentation are outlined below:

- It protects your high-value assets, such as Active Directory, file servers, or database servers. These assets, often dubbed, "crown jewels," are items threats actors will target first. By only having explicitly authorized systems/administrators reach these assets, along with the addition of monitoring tools, you can create a difficult time for threats actors to try and obtain this access.
- Without segmentation, it can be presumed that a stolen credential, depending on the level of access, can create a threat actor to start gaining access everywhere. With segmentation, each "hop" in your network would require additional entry.
- Ransomware-as-a-service (RaaS) can also be limited. Threat actors do rely on automated discovery and script-based deployments, and segmentation could force hosts to not enumerate across all networks/subnets. GPO-backed ransomware deployment scripts can also be dropped.

Cyber Hygiene – Offline *Backups*:

Considered a critical step in ransomware defense, offline backups can create an air-gapped copy of your imperative data that is disconnected from the network. This detachment can ensure that threat actors are unable to reach this data, which would prevent encryption, deletion, etc. Often, companies follow a ***3-2-1*** backup rule, which dictates keeping **three** copies of your data, on **two** different media type files, with **one** copy offsite.

Some providers in the backup field can include the following:

- Veeam.
- Acronis.
- Microsoft via Azure Backup.

Cyber Hygiene – *End User Training*:

We know that email is a steady attack vector for threat actors, and this makes end user security training a necessary element when it comes to defending your sensitive data. Studies have shown that regular training can reduce your risk of having a security incident by 50%. Educating your users about phishing, AI-inspired attacks, and ransomware prevention are all chief elements in strengthening a company's security posture.

Popular vendors for cybersecurity training can include:

- KnowBe4.
- Hoxhunt.
- Proofpoint.

Each listed vendor also offers complementary security blogs that track the latest trends and attacks that can significantly impact companies. Some vendors, such as KnowBe4, will also offer free tools for phishing tests, ransomware simulators, and email exposure checks.

Cyber Hygiene – *AV/EDR*:

Within the current cybersecurity landscape, it is ideal for companies to utilize AV (anti-virus) and/or EDR (endpoint detection response) tools inside their environment. The main difference between AV and EDR starts with initial access. Specifically, AV is more traditional, which will attempt to prevent malware from spreading at an entry point. On the other hand, EDR will continuously monitor all servers, devices, user activity, etc., behavior in real-time. This incessant monitoring allows for more robust inspection at detecting suspicious actions and/or anomalies.

EDR is more capable at stopping threats like ransomware since it offers around-the-clock eyes using AI, machine learning techniques, and UEBA (user and entity behavior analytics) to prevent/quarantine threats. This differs from conventional AV, as it tends to use known-bad signatures to do its blocking.

Some notable EDR vendors in the cybersecurity field can include:

- CrowdStrike Falcon.
- SentinelOne Singularity.
- Sophos Endpoint.
- Microsoft Defender.

Free solutions on the AV front for companies can include:

- Microsoft Defender.
- BitDefefender.
- Avast.
- Malwarebytes (anti-malware tool).

Cyber Hygiene – *Least Privilege*:

Probably one of the most overlooked security measures that a company could implement, least privilege centers around providing users only required permissions to do their jobs. In other words, users on the Finance Team only can see and access Finance-specific folders, applications, mailboxes, etc., as there is no real need for them to access HR-related data on the network.

When over-permissive access is present, you are left with an increased attack surface that can lead to not only malicious insider activity, but privilege escalation attempts that can allow threat actors to pivot throughout systems.

Cyber Hygiene – *Tabletop Exercises*:

Tabletop exercises are discussion-based scenarios in preparation for cyberattacks, such as ransomware. Companies can hold these exercises on a quarterly or yearly basis. The main concept of this type of practice is to simulate a cyberattack on your company. Participants can include all relevant personnel that can handle emergency-like plans, such as IT, HR, Senior Management, and Legal. To possibly conduct a tabletop, you can consider the following items:

- Define a set scope of plans.
- Develop a scenario that can include the disaster you want to simulate.

- Add the necessary players.
- Conduct the exercise.
- Hold an after-action review that allows all players to debrief the course of events, findings, and what went well/did not in the exercise.
- Create an action and/or lessons-learned plan on what to improve for the next tabletop.

Other Security Tips to Ponder?

- **Patch**, **patch**, **patch**! Out-of-date software is a breeding ground for cyberattacks to prosper. Ensure that end user applications and OS security updates are always present and deployed.
- Consider restricting **social media** and **personal-based email** websites that users can access. Social engineering is a legitimate threat and by blocking sites like the above, you can possibly reduce these types of attacks, while increasing your cybersecurity footprint.
- Practice **good password hygiene** with potentially adding 14-character password mandates and implementing a no-password reuse/variation policy.
- Think of adding a **password manager** to your company's environment. Password managers are resourceful security tools to keep passwords off your users' desktops, spreadsheets, and stored within their browsers.
- Have a **firewall** in place. Firewalls can be beneficial as a first line of defense since they monitor and control all inbound/outbound traffic via security policies. With a firewall you will be able to block certain applications, ports, websites, IP addresses, etc., with configured rules to keep threat actors potentially out.
- Establish **conditional access policies** when it comes to employee logins.
- Utilize a **VPN** on all endpoints.
- Implement **SSO/MFA** across your environment and on applications.

Statistics were derived from: Cisa.gov, Acronis.com, brside.com, csoonline.com, redcanary.com, pcmag.com, and microsoft.com.

Accredited sites to cross-check vendors, products, and to review ratings: https://www.gartner.com/peer-insights/home and https://www.capterra.com/p/253536/Checks/.

Disclaimer:
The information provided in this article is for informational purposes only and does not constitute professional advice. While the CATIC IT Security Department strives to share helpful cybersecurity insights, CATIC makes no representations or warranties regarding the accuracy, completeness, or suitability of this information for any environment and assumes no liability for actions taken based on this content. Agents are encouraged to consult their own IT department, managed service provider (MSP), internal technical staff, or qualified advisor(s) before making any cybersecurity decisions. We value our partnership and are committed to supporting your continued success.