(858) 999-3030 • www.rsisecurity.com • info@rsisecurity.com

Ransomware Prevention Checklist

- [x] **Protect your organization from ransomware attacks**

Install and Maintain Baseline Protections

- [ ]

The first line of defense against ransomware is establishing general cybersecurity protections across all your assets and devices.

For example, you should employ network segmentation, or physical or logical separations between assets and systems used for IT, business operations, and other purposes. Use antivirus or antimalware programs to track for, report on, and eliminate malicious software across your systems. And consider preventing all software from running or being installed unless it meets certain authorization criteria—a process known as application directory allowlisting.

Another fundamental practice is patch management, ensuring that configurations are updated as soon as possible and operating as expected.

Implement Advanced, Preventive Safeguards

- [ ]

Once you have a secure baseline in place, you'll want to build on protections specific to the kinds of hardware and software you use. Some advanced safeguards to consider include:

- Secure remote desktop protocol (RDP) restrictions, like IP limitation or gateway servers
- Web and content filters at email and other gateways to flag suspicious, unknown traffic
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies

In some cases, it might help to disable certain built-in settings like Server Message Block (SMB) protocols or macro scripts for email files. You should consult with a security program advisor to determine whether these or other solutions would be best suited for your organization.

Leverage Your Staff to Protect Against Ransomware

- [ ]

One of the biggest vectors for ransomware attacks comprises human targets, who may unintentionally or unwittingly install malware onto your systems.

However, it's important to note that staff can also be a resource. Train employees to cultivate awareness and vigilance so they're less likely to fall victim to an attack and more likely to report suspicious activity or traffic they come across. And implement access controls such as multifactor authentication (MFA) and the principle of least privilege to limit the damage that can be done even if their credentials are guessed, leaked, or stolen.

Beyond staff-wide measures, you should also pay special attention to position-specific weaknesses. Restrict access by business need to know, and closely monitor the uses and behaviors of staff in critical positions, such as those with access to domain controllers (DCs).

Data provided by CISA

(858) 999-3030 • www.rsisecurity.com • info@rsisecurity.com

Ransomware Prevention Checklist

Protect your organization from ransomware attacks

Monitor System Activity and Vulnerabilities

With system protections and an aware, vigilant staff in place, you'll want to install visibility infrastructure to monitor your networks. This includes comprehensive network diagrams that illustrate normal traffic and data flows and user activities within your systems. You should also log all access and user behavior, along with results of system-wide scans and assessments, securing this information for future backups, analysis, and threat intelligence.

Taken together, these kinds of practices allow you to identify regular system operations and behavior. Any irregularity or disturbance is a potential threat to mitigate.

Detect, Respond to, and Manage Threats

Beyond regular system monitoring for irregular behavior, you should also employ methods to scan for, detect, and respond to security events that do occur. Best practices include:

Threat and vulnerability management – Track and mitigate real and potential risks to your system before, during, and after they materialize into full-blown attacks.

Managed detection and response (MDR) – Use intrusion detection systems (IDS) and other continuous monitoring to detect and immediately respond to an attack.

Incident management – Prepare for short- and long-term recovery and business continuity with offline encrypted backups of sensitive data.

You also should monitor for and manage incidents across partners' and vendors' systems that connect to your own through third-party risk management (TPRM).

Optimize Your Ransomware Prevention

Finally, organizations should look to streamline all the practices above into efficient, optimized ransomware prevention. Ransomware controls work best when fully integrated with other cybersecurity protections, such as your Security Information and Event Management (SIEM) protocols or any framework controls implemented for regulatory compliance.

One of the most effective ways to do this is to work with a managed security service provider (MSSP), such as a security program advisor or virtual Chief Information Security Officer (vCISO).

Data provided by CISA