blackpoint

CHECKLIST

Offensive Checklist Against Ransomware

Fighting the threat of ransomware is an ongoing endeavor, but MSPs and their clients are far from helpless. This checklist outlines five effective best practices that both you and your clients can undertake to safeguard networks from ransomware attacks.

☐ Security Awareness and Training

Take time to provide routine cybersecurity awareness training, allowing employees to understand:

- How cybersecurity affects their own safety at work, not just the interests of the company.
- That they could unknowingly pass on or expose sensitive information if not trained or prepared.
- The importance of staying vigilant against social engineering tactics, phishing emails, and malicious links and attachments.

☐ Establish IT Cyber Hygiene

Set your business up for success by adopting tried and true cybersecurity hygiene practices.

- Ensure that patching and upgrade activities are completed particularly for firewall and VPN appliances.
- Establish app-based MFA (2FA at the least) for all devices and RMM tools.
- Remove internet-exposed remote desktop services (RDP) services.
- Lock up devices not in use and protect hard drives through encryption.
- Run regular vulnerability assessments against all systems on your network.

Implement an Effective Security Stack with Active Monitoring

Building and maintaining a security stack that provides adequate protection is one of the most important tasks for IT administrators. An elegant security stack will include:

- Endpoint protection technology,
- Backup and recovery technology,
- MFA capability,
- VPN or Zero Trust remote network access,
- Vulnerability management with patching, and
- 24/7 monitoring with active detection and response.

Establish Regular Backups

Backups are an integral element in any cybersecurity toolkit as it allows for business continuity in the event of a disaster or emergency. Key aspects of backup and disaster recovery (BDR):

- Scheduling regular backups that are offline and cloud based
- Ensuring backups are organized and frequently reviewed
- Protection through passwords and encryption

Implement Log Monitoring and MDR

Controlled and effective log monitoring helps you detect anomalies, detect threat patterns, and show you signs of exploitable areas in your networks. Logs are most effective when they are actively monitored by experienced Managed Detection & Response (MDR). Analysts can sift through complex logs, compile threat intelligence in real-time, and detain at the first sign of compromise.

Adopting an 'Assume Breach' Posture

Don't make it easy for threat actors to exploit your user accounts and move laterally in your networks. Nip their actions in the bud by implementing a principle of Zero Trust. This principle works by eliminating the concept of trust from the inherent architecture of your operations. Zero Trust does the following:

- Requires each user and machine authenticate before granting access,
- Segments networks so threat actors can be more easily detained before they further penetrate your systems, and
- Minimalizes exposure of your network's most sensitive or critical data.

We recommend that you map out the user roles needed to sustain your operations and then attribute the specific permissions each role needs to perform their associated tasks. Perform regular internal reviews of your accounts to revoke excessive permissions or deactivate accounts no longer in use.

Want to learn more about the around-the-clock security analysts and proprietary technology that can protect you from ransomware?

LEARN MORE ABOUT OUT MDR

blackpoint

blackpointcyber.com