TEVORA™

Top 5 Strategies for Avoiding Ransomware Attacks

With ransomware attacks on the rise, it's more important than ever to prepare your staff and systems to defend against these potentially devastating incidents. **Here are our top five strategies for avoiding ransomware attacks.**

1. Evaluate your threat profile

Perform an assessment to identify, validate, and provide remediation steps for any vulnerabilities in your environment that can be exploited by potential ransomware attacks. Techniques such as Red Teaming, Purple Teaming, and penetration testing can simulate real-world ransomware attacks using the latest ransomware payloads and attack vectors to identify vulnerabilities.

2. Review and update your security controls

Conduct an Enterprise Ransomware Risk Assessment to identify ransomware-related risks and determine if your current security controls are adequate to address these risks. If not, update your security controls and any related policies and procedures to ensure all malware-related risks are covered.

3. Know your data

Ensure that you understand where your data is stored, how it's used, and how it may be vulnerable to ransomware attacks. If you don't already have a current map of your data, we recommend performing a detailed mapping exercise to document where each data element is stored, who has access to it, where it comes from, how it flows through your organization, and who it is shared with. We also recommend performing a privacy impact assessment to understand where your sensitive information is stored, how it is used, and what security controls are in place to protect it.

4. Implement a "Zero Trust" Architecture

As companies increasingly move to hybrid environments where applications and data are spread across on-premise and cloud environments, traditional approaches focused on defending the in-house network perimeter are becoming obsolete. We recommend implementing a Zero Trust architecture to strengthen your defenses against ransomware and other external attacks. With this approach, every device or person accessing a company resource is verified, regardless of whether they are inside or outside the in-house network perimeter. This broad concept includes elements such as multi-factor authentication (MFA), granular network segmentation, and "least privilege" access rights and privileges.

5. Have an Incident Response Plan

Develop an incident response plan that identifies the people, processes, communications plans, technical solutions, and other resources that will be deployed to detect and respond to ransomware attacks. We recommend having in-house or third-party ransomware experts identified and ready to respond when an incident occurs. Key skills these experts should have include ransomware detection and analysis, emergency incident response management, communication with criminal ransomware organizations, ransomware eradication, and restoration of normal operating environments.

Tevora's Ransomware Preparedness Services can help ensure your organization is ready for ransomware attacks.

If you have questions about ransomware or would like our help preparing your organization for these attacks, just give us a call at (833) 292-1609 or email us at sales@tevora.com.

tevora.com