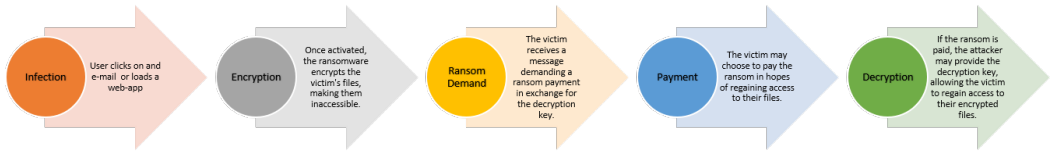
Ransomware Best Practices

Dont let ransomware break your company!

Ransomware is a type of malware that encrypts files on a device, making them and the systems that rely on them unusable. Attackers then demand a ransom in exchange for decryption. Over time, these malicious actors have evolved their tactics, sometimes even threatening to release stolen data, a strategy known as “double extortion.” Ransomware attacks have seen a significant rise, with a 13% increase year-over-year from 2021, surpassing the growth of the previous five years combined. Small businesses reported 832 ransomware-related data breaches in 2022, with 130 confirming data loss. Nearly 80% of these attacks were due to ransomware. While small business losses are often not reported, it is estimated that small businesses pay an average of $200,000 per incident.

The Ransomware Process



- **Preparation**: Maintain offline, encrypted backups of critical data and test them regularly. Use “golden images” of critical systems for quick deployment in case of attacks. Consider multi-cloud solutions for backups.
- **Access Control:** Implement a zero-trust architecture, ensuring granular access control. This assumes the network is compromised and aims to minimize uncertainty in access decisions.
- **Vulnerability Management:** Regularly scan for vulnerabilities, especially on internet-facing devices. Patch and update software and operating systems promptly.
- **Credential Management:** Implement phishing-resistant multi-factor authentication (MFA) for all services. Use strong password policies and consider using password managers. Monitor for compromised credentials on the dark web.
- **Phishing Prevention:** Educate employees on identifying and reporting phishing attempts. Implement email filters to block known malicious indicators and use Domain-based Message Authentication, Reporting, and Conformance (DMARC) to prevent email spoofing.
- **Malware Prevention:** Use updated antivirus and anti-malware software. Some ransomware attacks are a result of existing malware infections, so detecting precursor malware is crucial.

+1.619.508.8871
www.tracc.com
info@tracc.com

TRACC DEVELOPMENT, INC

Ransomware: The response checklist.

1. **Immediate Actions:**
   - Isolate affected systems to prevent the spread of ransomware.
   - Secure backup data or systems by ensuring they are offline and not accessible from compromised networks.
   - Notify organizational leadership and activate the incident response team.

2. **Engage with Law Enforcement:**
   - Report the incident to law enforcement agencies, such as the FBI or CISA, to get assistance and guidance. (Authors' note: Many companies are insecure about inviting the FBI or CISA in, thinking that it will open up a wider investigation of the company. This is not the case. Unless you are running a blatantly illegal operation, there is little risk and high possible benefit.)

3. **Assess the Situation:**
   - Determine the scope of the incident, including which systems and data are affected.
   - Identify the strain of ransomware used in the attack.
   - Check for a ransom note and follow organizational procedures on whether to engage with the threat actor.

4. **Engage External Stakeholders:**
   - Notify external stakeholders, such as partners, customers, or regulatory bodies, if their data is affected.
   - Engage with external cybersecurity professionals for incident response and recovery.

5. **Recovery:**
   - Restore systems from clean backups after ensuring the ransomware has been completely removed.
   - Validate the integrity of the restored data.
   Implement security measures to prevent future attacks.

6. **Post-Incident Activities:**
   - Conduct a post-incident review to identify lessons learned and areas for improvement.
   - Update incident response and business continuity plans based on the findings.
   - Train employees on ransomware awareness and prevention.

7. **Continuous Monitoring:**
   - Monitor network traffic and system logs for signs of malicious activity.
   - Update and patch systems regularly.
   - Implement advanced threat detection and response solutions.