Comtrade Three-Sixty

Comprehensive Ransomware Prevention and Response Checklist

Proactive and Reactive Measures to Combat Ransomware Threats

Ransomware attacks have become a pervasive threat in today's digital landscape, targeting organizations of all sizes and across various industries. These malicious attacks can disrupt operations, compromise sensitive data, and result in significant financial losses. At Comtrade 360, we understand the critical importance of safeguarding your organization's assets and ensuring business continuity. This comprehensive ransomware prevention and response guide provides detailed, actionable steps to fortify your defenses and prepare for effective incident management. By following this guide, you can enhance your cybersecurity posture, minimize the risk of ransomware attacks, and ensure a swift and efficient recovery if an incident occurs.

Ransomware Prevention and Response Checklist

PREVENTION

- □ **Security Awareness Training:**
  - □ Educate end users about ransomware attacks and safe practices.
  - □ Train end users to spot and report phishing emails with malicious attachments.

Software-Level Preventive Measures

- □ **Firewalls:**
  - □ Ensure firewalls are always operational and up-to-date.
- □ **Network Segmentation:**
  - □ Logically separate networks to contain potential threats.
- □ **Email Filtering:**
  - □ Employ a strong email filtering system to block spam and phishing emails.
  - □ Implement advanced email filtering solutions to block malicious attachments and links.
  - □ Deploy anti-phishing tools that identify and block phishing attempts.
- □ **Software Restriction Policies:**
  - □ Set up rigorous policies to block unauthorized programs from running.

- □ **Antivirus and Anti-Malware:**
  - □ Ensure antivirus software is fully operational and up-to-date.
  - □ Install and maintain updated antivirus and anti-malware software on all endpoints.
- □ **Patch Management:**
  - □ Ensure all operating systems are up to date with the latest patches.
  - □ Keep all software applications, including third-party apps, updated.
  - □ Use patch management tools to automate the deployment of updates.
- □ **Intrusion Detection Systems (IDS):**
  - □ Use a strong, real-time intrusion detection system to spot potential attacks.
  - □ IDeploy IDS/IPS to monitor and respond to suspicious activities.
- □ **Remote Desktop Protocol (RDP):**
  - □ Disable RDP when not in use.
- □ **Macros in Office Files:**
  - □ Disable macros in Microsoft Office files.
- □ **Security Assessments:**
  - □ Conduct periodic security assessments to identify vulnerabilities.
- □ **Access Controls:**
  - □ Ensure users have the minimum level of access necessary for their roles.
  - □ Enforce MFA for accessing critical systems and sensitive data.
  - □ Regularly review and update user accounts and permissions.

Backup-Level Preventive Measures

□ **3-2-1 Backup Rule:**

- □ Follow the 3-2-1 backup rule: retain three copies of data on two different storage types, with one copy stored offline.

□ **Periodic Backup:**

- □ Ensure periodic backups of critical work data.

□ **Data Integrity Checks:**

- □ Enforce regular checks for data integrity and recovery on all backups.

□ **Automated Backups:**

- □ Implement automated backup systems to ensure regular backups.

□ **Backup Storage:**

- □ Store backups in multiple locations, including offline and offsite.
- □ Use encrypted storage to protect backup data.

□ **Backup Testing:**

- □ Regularly test backup restoration to ensure data integrity and reliability.

DETECTION

□ **Monitoring**

- □ Continuously monitor network traffic for unusual patterns or activities.
- □ Deploy SIEM solutions to aggregate and analyze security event data.
- □ Use behavioral analysis tools to detect anomalies in user and system behavior.

□ **Alerts**

- □ Configure automated alerts for suspicious activities, such as unauthorized access attempts, unusual file encryption, and large data transfers.
- □ Prioritize alerts based on severity and potential impact.
- □ Develop and maintain response playbooks for common alert scenarios.

RESPONSE

Time-Sensitive Reactive Measures

□ **Immediate Shutdown:**

- □ Shut down infected systems immediately. and reliability.

□ **Isolation:**

- □ Disconnect and isolate infected systems from the network.
- □ Isolate backups immediately.
- □ Disable all shared drives that hold critical information.

□ **Alerts:**

- □ Issue an organization-wide alert about the attack.

□ **Law Enforcement:**

- □ Contact local law enforcement and report the attack.

Analysis-Based Reactive Measures

□ **Scope and Magnitude:**

- □ Determine the scope and magnitude of the infection by identifying infected devices and encrypted data.

□ **Ransomware Identification:**

- □ Determine the type and version of the ransomware. s and encrypted data.

□ **Threat Vector Identification:**

- □ Identify the threat vector used to infiltrate the network.

□ **Root Cause Analysis:**

- □ Conduct root cause analysis to identify how the attack occurred.

□ **Mitigation:**

- □ Mitigate any identified vulnerabilities.

□ **Decryption Tools:**

- □ Check if a decryption tool is available online for the specific ransomware.

Business Continuity Reactive Measures

□ **Restore from Backup:**

- □ Restore files from a verified and clean backup.

MAINTENANCE

□ **Regular Testing**

- □ Regularly test backup and restoration procedures to ensure reliability.
- □ Conduct periodic penetration tests to identify vulnerabilities.
- □ Perform regular vulnerability assessments to keep systems secure.

□ **Policy Updates**

- □ Regularly review and update security policies and procedures.
- □ Ensure policies comply with the latest regulations and industry standards.

□ **Continuous Improvement**

- □ Stay informed about the latest ransomware threats and mitigation techniques.
- □ Participate in cybersecurity forums and information-sharing groups.
- □ Encourage continuous training and certification for IT and security staff.

Comtrade 360 Security Services

Penetration Testing

Comtrade 360's Penetration Testing services rigorously simulate cyber attacks to identify and address vulnerabilities in your network, cloud, and application infrastructure. Our expert team employs advanced techniques to uncover potential security gaps, providing detailed reports and remediation guidelines to strengthen your defense mechanisms. By proactively identifying risks, we help you ensure compliance, protect critical assets, and maintain stakeholder confidence.

Security Assessment

Our Security Assessment services offer a comprehensive evaluation of your ICS/OT and overall cybersecurity posture. We identify vulnerabilities, assess risks, and provide actionable recommendations to safeguard your critical infrastructure. With a focus on regulatory compliance and increased resilience, our assessments empower you to manage risks effectively, ensure business continuity, and educate employees on best security practices.

DevSecOps

Comtrade 360's DevSecOps solutions integrate security seamlessly into your development lifecycle. By combining SAST, DAST, and IAST tools, we detect vulnerabilities early and enhance code quality through continuous testing and monitoring. Our approach ensures that security is an integral part of your CI/CD pipeline, reducing the risk of breaches and optimizing your development process for faster, more secure releases.

Managed Services

Our Managed Services provide ongoing maintenance, monitoring, and updates for your CI/CD and security infrastructure. Our skilled engineers ensure uninterrupted development by keeping your systems up-to-date and secure. Regular updates, patch management, and continuous optimization of pipelines and monitoring tools help you focus on development while we handle the infrastructure, ensuring efficiency and security at all times.

Comtrade
Three-Sixty

info@comtrade360.com
+1 617-546-7400
comtrade360.com