What to Do in the First Hour of a Ransomware Attack

A Step-by-Step Guide to Immediate Containment and Response

When ransomware strikes, the first hour is crucial. Taking the right actions can significantly reduce damage and accelerate recovery. Follow these steps:

1. Isolate to Contain the Damage

Immediately disconnect infected systems from the network, Wi-Fi, and shared drives. If a device appears suspicious, lock it down. Ransomware spreads quickly, so containment must be prioritized over investigation.

☑

2. Cut Off Shared Access Points

Disable shared folders, cloud synchronization tools (like OneDrive or Dropbox), and remote desktop protocols (RDP). This prevents the attack from reaching additional connected users or environments.

☑

3. Preserve Evidence for Forensics

Do not reboot, wipe, or reimage infected systems. Instead, preserve logs, memory dumps, and system states for your incident response or forensics team. This data is essential for identifying how the breach occurred.

☑

4. Activate Your Incident Response Team

Immediately alert your internal or external Incident Response (IR) team. If you don't have one, contact a cybersecurity partner experienced in ransomware recovery. Quick action is vital—get experts involved immediately.

☑

5. Initiate Your Incident Response Plan (IRP)

Follow your predefined IRP procedures, which include assigning roles, communicating with stakeholders, and documenting every decision. If you lack a plan, escalate the matter to leadership and treat the situation as a live-fire drill.

☑

6. Involve Legal and Compliance Teams Early

Engage your legal counsel and compliance officers as soon as a ransomware incident is suspected. You may have regulatory obligations for breach disclosure depending on the data affected and your jurisdiction.

☑

7. Document Everything in Real-Time

Record key details as they unfold, including:

- Who discovered the incident
- The systems involved
- Timestamps and screenshots
- All actions taken and by whom

Thorough documentation supports legal defenses, insurance claims, and post-mortem analysis.

☑

8. Do Not Engage the Attacker

Never respond to ransom notes or initiate payment discussions without guidance from legal and your IR team. Engaging with attackers can exacerbate the situation or even pose legal risks, depending on the group's affiliations.

☑

Pro Tip: Even the best response cannot compensate for a lack of preparation. Test your IR plan, train your staff, and collaborate with a cybersecurity partner to stay ahead of emerging ransomware threats.

cyberclan.com