5 TIPS *for* INCIDENT RESPONSE

Incident response is the practice of having plans and strategies in place should a cyberattack penetrate an organization's defenses. Think of it as a counterattack against the perpetrators. With a formal, tested incident response plan, you can rapidly detect breaches, minimize damage and quickly restore normal operations.

These five tips will help you devise an effective incident response plan.

TIP ONE

Identify and Prioritize Assets

Identify and document the locations of your crucial data and other assets. Assess if backups are available. Prioritize the protection and recovery of these assets according to their significance.

This practice is essential to mitigating damage in the wake of a cyberattack since **60% of companies shut down within six months of a successful cyberattack**.

TIP TWO

Determine Potential Risks

Perform a risk assessment to check for vulnerabilities in your systems and network. Assessing risk is vital since threats like ransomware, business email compromise (BEC), phishing and distributed denial of service (DDoS) can have severe consequences on an organization. Today, **the average cost of a ransomware-related data breach is estimated at $4.54 million**.

TIP THREE

Set Up Breach Plans and Procedures

Create a streamlined plan that covers all elements in the incident response cycle. Confused employees are the last thing you need during a security incident. Without a written formal plan in place, employees are likely to commit security blunders that might be detrimental to the organization.

TIP FOUR

Build a Strong Incident Response Team

Form an incident response team that can rapidly respond to a cyberattack, efficiently coordinate your organization's post-breach actions and restore operations as quickly as possible. Each member of the team should understand their particular role in the plan and have proper communication channels to collaborate during and after an incident.

TIP FIVE

Train Your Employees

Ensure your employees are aware of the incident response plan, explain why it exists and provide the necessary training for them to successfully enact it. The success of your incident response plan hinges on its effective execution. Organizations that engage their employees in regular security awareness training experience **70% fewer security incidents**.

Detect and Mitigate Incidents Rapidly with Managed SOC

A Security Operations Center (SOC) offers expert monitoring of your network 24/7 to detect and mitigate cyberattacks timely and effectively without adding to your payroll.

Kaseya Managed Security Operations Center (SOC) offers round-the-clock monitoring of your networks and systems without the expense and hassle of setting up an in-house SOC. Our cybersecurity experts leverage our Threat Monitoring Platform to detect and mitigate malicious and suspicious activities across three critical attack vectors: endpoints, networks and cloud.

LEARN MORE