PorteBrown ACCOUNTANTS & ADVISORS

Ntiva Managed IT, Security, & Cloud Services

HACK ACTION PLAN

Step 1: Confirm the attack

Check if your computers or networks have been compromised. If you have log files, this is the ideal starting place. Symptoms of a breach include defacement, an extortion attempt, systems behaving abnormally, or malicious files found on your servers. Skilled attackers attempt to cover their tracks and deletion of log files is a common practice.

Step 2: Contain the attack

When investigating security breaches, valuable "volatile data" is lost when systems are powered down, including RAM contents and active network connection. Consult a security expert (depending upon the type of attack), because it is important to fully understand the options and ramifications when determining your initial response. Having backups are critical at this step. It is critical to review basic security policies like password age and complexity. Also reviewing your user accounts to make sure everyone that has an account is still an active employee. Two to four weeks for this step is not out of the ordinary.

Step 3: Understand and investigate the attack

Investigate how deep the hacker penetrated into your systems and networks and what was accessed, stolen or destroyed. Making sure you send your log files offsite is critical. If you access effected systems, use a "forensic write block" to preserve the systems untampered and able to be used in court.

Step 4: Report the attack

Depending upon the type of breach and level of risk, you may need to report the attack to the FBI. Money laundering, extortion or other forms of financial fraud must be reported immediately to the local authorities. You should also report the incident to the FBI.

Step 5: Determine the cause

You must pinpoint how the attacker first penetrated your network. Identifying the first point of entry is critical. Often hackers will leave doors open in order to regain access. It is critical to find out if the hackers can still access your systems while you're initiating recovery.

Step 6: Do you need to communicate the attack?

Determine how you will communicate with affected employees, vendors, customers, and partners about what transpired, what remediation steps you are taking, and what they need to do. In some cases, proper communication is mandated by law. Even when not required by law, timely and open communication may be a necessary salvage step for your business, since too many companies try to hide the attack only to permanently lose the trust of their customers and partners.

Step 7: Remediation

Develop a Business Continuity Plan (BCP) for increasing your IT security so you can identify and defend against future attacks. Make sure your applications and operating systems are current, patched and receiving automatic updates to fix bugs. Risky web applications may warrant having a Web Application Firewall in front of them to protect against web-based attacks.

Step 8: Proactive Security Protection

There is a quantifiable advantage and improved ROI on IT security budgets if you develop a plan for monitoring, investigating, and remediating. *After* the attack has been identified and mitigated, move your focus from reactive issues and crisis management to proactive security protection. Faster correlation of data patterns greatly reduces the financial and organizational impact of cybercrime on an organization. Prevention will come down to people, processes and technology all working together to keep you safe.

Porte Brown LLC | 845 Oakton St. | Elk Grove Village, IL 60007 | *p:* 847.956.1040 | *f:* 847.956.6780

Ntiva, Inc. | 5410 Newport Drive Unit 28 | Rolling Meadows, IL 60008 | *p:* 847.897.1640 | *f:* 847.786.8830

PorteBrown.com

Ntiva.com